Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра казахского и русского языков

РУССКИЙ ЯЗЫК

Методические указания и варианты семестровых работ для студентов специальностей 5В070400, 5В100200

Алматы 2016

СОСТАВИТЕЛЬ: Курманбаева Т.С. Русский язык. Методические указания и варианты семестровых работ для студентов специальностей 5В070400, 5В100200. – Алматы, АУЭС, 2016. – 66 с.

В данную методическую разработку включены задания к шести семестровым работам, перечень источников, варианты текстов, список периодических изданий для их выполнения.

Методические указания предназначены для студентов бакалавриата дневной формы обучения специальностей: 5В070400 – Вычислительная техника и программное обеспечение, 5В100200 – Системы информационной безопасности.

Библиогр. – 24 назв.

Рецензент: канд. фил. наук Кубдашева К.Б.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2015 г.

Введение

Предлагаемые методические указания и варианты семестровых работ студентов составлены согласно типовой учебной программе дисциплины «Русский язык» (объем – 6 кредитов).

Основная цель выполнения СРС заключается в выявлении уровня овладения обучающимися различными видами лингвистического анализа и продуцирования учебно-научных текстов, предусмотренных рабочей программой дисциплины, в виде шести письменных работ.

В методических указаниях сформулированы темы, указаны цели и задачи всех семестровых работ; представлены варианты текстов для анализа, списки рекомендуемой учебно-научной литературы и образец оформления титульного листа СРС.

Требования, предъявляемые к выполнению СРС

1. Семестровая работа должна быть выполнена в соответствии с графиком выдачи и приёма СРС.

2. Семестровая работа должна быть выполнена компьютерной вёрсткой шрифтом TimesNewRoman, кегль 14, одинарным междустрочным интервалом, в текстовом редакторе «MS Word». Абзацы в тексте начинают отступом для первой строки – 1,25 см, слева и справа – 0 см. Размеры полей: верхнее - 2 см, нижнее – 2,5 см, левое – 2,5 см, правое - 1,8 см. Страницы текста семестровой работы нумеруются вверху справа(подробную информацию об оформлении см. Lib.aipet.kz).

3. В конце работы должен быть приведён список использованной литературы и интернет-ресурсов. Последние ссылки должны быть конкретными с указанием даты обращения. Ссылки типа www.yandex.ru или www.google.ru не являются корректными.

4. В случае обнаружения плагиата к студенту могут быть применены санкции по усмотрению преподавателя (вплоть до аннулирования положительных результатов и получения оценки «неудовлетворительно» без права повторной сдачи).

Семестровая работа студента № 1

Тема: функционально-смысловые типы речи.

Цель: проявить навыки различения функционально-смысловых типов речи (описание, повествование, рассуждение).

Задачи работы:

- подобрать 3 текста, относящиеся к трем функционально-смысловым типам речи;
- указать 2-3 признака конкретного типа речи в каждом тексте;

- составить толковый словарь незнакомых лексических единиц по каждому тексту (из каждого текста не менее 10-ти слов).

Рекомендуемая литература для выполнения СРС № 1

1 Русский язык: учебное пособие для студентов казахских отделений университета (бакалавриат)/ Под ред. К.К.Ахмедьярова, Ш.К.Жаркынбековой. –Алматы: Қазақ университеті, 2009.– 226 с.

2 Мухамадиев Х.С. Пособие по научному стилю речи: для казахских отделений университета. -3-е изд. – Алматы: Қазақ университеті, 2011.- 210 с.

3 Тусипбек М.Р., Кусаинов А.К.. Русско-казахско-английский политехнический словарь: в 2-х томах. – Алматы: Rond&A, 2010.

4 Даль В.И. Большой иллюстрированный толковый словарь русского языка: современное написание. Около 1500 илл. – М.: «АСТ – Астрель - Хранитель», 2008. – 352 с.

Семестровая работа студента № 2

Тема: структурно-смысловой анализ текста по специальности.

Цель: показать умение анализировать структурно-смысловое строение научного текста.

Задачи работы:

- определить тему текста, выразив ее словом-темой и обозначив буквой Т;
- определить коммуникативную задачу текста, в которой заключена данная информация текста, обозначив ее аббревиатурой «КЗТ»;
- сделать анализ реализации КЗТ путем деления на микротемы (МТ1, МТ2, МТ3 …);
- выделить в тексте одно ССЦ (сложное синтаксическое целое) и определить способы связи предложений в нем (параллельная и цепная).

Тексты для выполнения СРС № 2 и № 3 специальности 5В070400 – Вычислительная техника и программное обеспечение

Вариант 1

Эволюция операционных систем

С момента появления первых вычислительных систем техническое и программное обеспечения эволюционировали совместно, оказывая взаимное влияние друг на друга. Появление новых технических возможностей приводило к прорыву в области создания удобных, эффективных и безопасных программ, а свежие идеи в программной области стимулировали поиски новых технических решений.

Программирование первых ламповых вычислительных устройств (1945–1955 гг.) осуществлялось исключительно на машинном языке. Об операционных системах не было и речи, все задачи организации вычислительного процесса решались вручную каждым программистом с пульта управления. При этом существенная часть времени уходила на подготовку запуска программы, а сами программы выполнялись строго последовательно (режим последовательной обработки данных). В результате исследований и разработок появляется первое системное программное обеспечение: в 1951–1952 гг. возникают прообразы первых компиляторов с символических языков (Fortran и др.), а в 1954 г. Нат Рочестер разрабатывает Ассемблер для IBM-701.

В середине 50-х годов одновременно с появлением транзисторов наблюдается бурное развитие алгоритмических языков, появляются первые настоящие компиляторы, редакторы связей, библиотеки математических и служебных подпрограмм. Для повышения эффективности использования компьютера задания с похожими ресурсами начинают собирать вместе, создавая *пакет* заданий. Появляются первые *системы пакетной обработки*, которые просто автоматизируют запуск одной программы из пакета за другой и тем самым увеличивают коэффициент загрузки процессора. При реализации систем пакетной обработки был разработан формализованный язык управления заданиями, с помощью которого программист сообщал системе и оператору, какую работу он хочет выполнить на вычислительной машине. Системы пакетной обработки стали прообразом современных операционных систем и первыми системными программами, предназначенными для управления вычислительным процессом.

Переход к интегральным микросхемам (начало 60-х – 1980 гг.) привел к увеличению сложности и количества задач, решаемых компьютерами. Пакетные системы начинают заниматься планированием заданий: в зависимости от наличия запрошенных ресурсов, срочности вычислений и т.д. на счет выбирается то или иное задание. Появление *мультипрограммных систем* обеспечило более эффективное использование системных ресурсов, но еще долго операционные системы оставались пакетными.

Логическим расширением систем мультипрограммирования стали системы *разделения времени* (time-sharing system), в которых процессор переключается между задачами не только на время операций ввода-вывода, но и просто по прошествии определенного времени. Эти переключения происходят так часто, что пользователи могут взаимодействовать со своими программами во время их выполнения, то есть интерактивно. В результате появляется возможность одновременной работы нескольких пользователей на одной компьютерной системе. Использование механизмов виртуальной памяти позволило создать иллюзию неограниченной оперативной памяти. В системах разделения времени пользователь получил возможность эффективно производить отладку программы в интерактивном режиме и записывать информацию на диск непосредственно с клавиатуры. Появление on-line-

файлов привело к необходимости разработки развитых файловых систем. В этот же период появилась идея стандартизации операционных систем.

Вариант 2

Устройство Flash

Flash-память – вид энергонезависимой, перезаписываемой полупроводниковой памяти. В основе этого типа флеш-памяти лежит НЕ-ИЛИ элемент (англ. NOR), потому что в транзисторе с плавающим затвором низкий уровень электронов обозначает единицу.

Транзистор имеет два изолированных затвора: управляющий и плавающий. Последний способен удерживать электроны в течение нескольких лет. В ячейке имеются так же сток и исток. При программировании между ними, вследствие воздействия положительного поля на управляющем затворе, появляется поток электронов.

Устройство Flash имеет довольно сложную структуру: процессы перепрожига микросхемы (flashing) базируются на законах квантовой механики. В простом случае ячейка Flash состоит из одного полевого транзистора. Элемент включает в себя специальную электрически изолированную область, называемую «плавающим затвором». Потенциал этой области не является стабильным, что позволяет накапливать в ней электроны (именно здесь и хранится вся информация памяти). Выше «плавающего» находится управляющий затвор, который является неотъемлемой частью при процессе записи/стирания данных памяти. Эта область напрямую соединена с линией слов. Перпендикулярно этой линии располагается линия битов, которая соединена со стоком (при записи данных из этой области транзистора появляется поток электронов). Сток разделяется с истоком специальной подложкой, которая не проводит электрический ток.

Запись данных во Flash происходит методом инжекции «горячих» электронов, а стирание – методом туннелирования Фаулера-Нордхейма: при программировании на сток и управляющий затвор подается высокое напряжение (причем, на управляющий затвор напряжение подается приблизительно в два раза выше. «Горячие» электроны (электроны называются «горячими» за то, что они обладают высокой энергией, достаточной для преодоления потенциального барьера, создаваемого тонкой пленкой диэлектрика) из канала инжектируются на плавающий затвор и изменяют вольт-амперные характеристики транзистора таким образом, что при обычном для чтения напряжении канал не появляется, и тока между истоком и стоком не возникает. При стирании высокое напряжение подается на исток. На управляющий затвор (опционально) подается высокое отрицательное напряжение. Электроны туннелируют на исток.

Флеш-память наиболее известна применением в USB флеш-носителях (англ. USB flash drive). В основном применяется NAND тип памяти, которая

подключается через USB по интерфейсу USB mass storage device (USB MSC). Данный интерфейс поддерживается всеми ОС современных версий.

Благодаря большой скорости, объёму и компактным размерам USB флеш-носители полностью вытеснили с рынка дискеты. Например, компания Dell с 2003 года перестала выпускать компьютеры с дисководом гибких дисков.

В данный момент выпускается широкий ассортимент USB флеш-носителей, разных форм и цветов. На рынке присутствуют флешки с автоматическим шифрованием записываемых на них данных.

Вариант 3

Возможности современной вычислительной техники

Возможности современной вычислительной техники, обусловленные ее техническими характеристиками, позволяют использовать ее во многих отраслях народного хозяйства для решения сложных задач, в свою очередь это обстоятельство требует разработки более сложного программного обеспечения. Увеличение парка ЭВМ определяет непрерывный рост числа организаций и специалистов, занимающихся разработкой программ прикладного характера.

Возможности современной вычислительной техники и устройств сопряжения с объектом позволяют решать задачу структурной и параметрической идентификации в реальном времени, используя компьютер и как устройство, генерирующее различные тестовые сигналы, и как устройство, обрабатывающее сигналы отклика исследуемого объекта. Таким образом, исследуемый объект и компьютер образуют, замкнутый контур, что позволяет осуществить взаимную привязку во времени входных и выходных сигналов. Подобное автоматизированное рабочее место исследователя систем управления (АРМ ИСУ) позволяет в интерактивном режиме проводить испытания, использовать различные методы обработки экспериментов, строить и анализировать модели по определенной методике фактически от эксперимента к эксперименту, уточняя и усложняя получающуюся модель.

Первое - специалист должен знать и уметь использовать *возможности современной вычислительной техники*, включая освоение языков программирования, с тем, чтобы уметь самостоятельно составлять программы для обработки результатов экспериментов, производить расчеты по дипломному и курсовому проектированию.

Несмотря на весь огромный арсенал методов анализа, проблема обработки информации, превращения ее из множества неупорядоченных фактов в систему, которую можно определить как истинные знания, остается чрезвычайно сложной и в общем случае нерешенной. Парадоксально, но *возможности современной вычислительной техники* создают даже своеобразный тупик.

Возникший разрыв между достижениями науки и инженерной практикой требует создания современных нормативных методик - инженерных методов нового поколения, учитывающих основные закономерности загрязнения окружающей среды, *использующих возможности современной вычислительной техники*, экспериментального моделирования и предназначенных для пользователей-непрофессионалов.

Современная вычислительная техника позволяет точно решать многие задачи, от решения которых раньше приходилось отказываться. Использование вычислительной техники идет в настоящее время по двум основным направлениям:

- вычисления выполняются на цифровых вычислительных машинах по старым алгоритмам, приспособленным к новым условиям;

- разрабатываются новые методы теории управления, рассчитанные на *возможности современной вычислительной техники*. Примером второго направления может служить структурная схема ЭВМ, где предлагаются новые матричные методы расчета устойчивости, не связанные с построением характеристического полинома и рассчитанные на использование цифровых электронных вычислительных машин.

Вариант 4

Методы передачи сообщений

Наиболее распространенными техническими средствами информирования в коммуникациях являются системы радиовещания и телевидения. Часто наиболее важная информация, необходимая очень широким деловым кругам, поступает именно через эти системы: сведения о принятии новых положений и законов, постановления правительств, курсы валют, курсы ценных бумаг и т.д. На массового потребителя рассчитана трансляция рекламных материалов. Если передача телевизионных программ сопровождается текстовой информацией, которая может быть рассчитана на прием обычным телевизионным приемником или приемником, оснащенным специальной аппаратурой, то говорят, что приемник имеет режим приема телетекста. При приеме такой программы на экране телевизора вместо обычных изображений высвечивается текст, как на экране монитора персонального компьютера.

Однако в деловом общении гораздо более важной может оказаться необходимость передать партнеру какую-либо информацию, имеющую частный характер, т.е. не рассчитанную на широкую аудиторию. Для этого имеется широкий набор технических средств, относящихся к классу средств так называемой *документальной электронной связи*. Такой тип электросвязи предназначен для передачи сообщений, представленных в форме документов, т.е. буквенно-цифровых текстов, рукописей, чертежей, рисунков, фотографий и т.п. Можно выделить две большие группы таких средств, отличающиеся

используемыми методами передачи сообщений: с факсимильным и кодовым методами передачи.

Ф а к с и м и л ь н ы й м е т о д передачи сообщений предполагает непосредственную передачу изображения документа с помощью специальных аппаратов – *телефаксов,* или просто *факсов,*

При передаче к о д о в ы м м е т о д о м производится посимвольное кодирование сообщений – как текстов, вводимых в персональный компьютер непосредственно с клавиатуры, так и графических файлов, т.е. соответствующим образом закодированных изображений (чертежей, рисунков, фотографий и т.п.). К последним относятся также файлы, полученные в результате обработки документов (например, стандартного листа бумаги с текстом официального письма, подписями и печатью) с помощью специальных устройств, называемых сканерами эти устройства предназначены для получения электронной копии любого документа.

В качестве технических средств, реализующих кодовый метод передачи сообщений, в настоящее время наиболее широко используются персональные компьютеры с соответствующим программно-аппаратным обеспечением, часто объединенные в компьютерные сети. Связь между различными компьютерами в сети, а также между компьютерными сетями осуществляется с помощью телекоммуникационных каналов – медных проводов, оптических волокон, радиоканалов (как наземных, так и спутниковых). Компьютерные сети могут включаться в мировую компьютерную сеть Интернет (Internet). На базе таких технических средств основаны чрезвычайно распространенные сейчас системы электронной почты, компьютерных досок объявлений, телеконференций, пейджинговой связи и т.п.

Вариант 5

Развитие науки на протяжении XX века

XX век стал веком победы научной революции. НТП ускорился во всех развитых странах. К середине XX века фабричный способ производства стал доминирующим. Во второй половине XX века большое распространение получила автоматизация. К концу XX века развились высокие технологии, продолжился переход к информационной экономике. Все это произошло благодаря развитию науки и техники. Это имело несколько последствий.

Во-первых, увеличились требования к работникам. От них стали требоваться большие знания, а также понимание новых технологических процессов. Во-вторых, увеличилась доля работников умственного труда, научных работников, то есть людей, работа которых требует глубоких научных знаний. В-третьих, вызванный НТП рост благосостояния и решение многих насущных проблем общества породили веру широких масс в способность науки решать проблемы человечества и повышать качество жизни. Эта новая вера нашла свое отражение во многих областях культуры и общественной мысли. Такие достижения: как освоение космоса, создание

атомной энергетики, первые успехи в области робототехники, породили веру в неизбежность научно-технического и общественного прогресса, вызвали надежду скорого решения и таких проблем как голод, болезни и т.д.

И на сегодняшний день мы можем сказать, что наука в современном обществе играет важную роль во многих отраслях и сферах жизни людей. Несомненно, уровень развитости науки может служить одним из основных показателей развития общества, а также это, несомненно, показатель экономического, культурного, цивилизованного, образованного, современного развития государства. Наука была актуальна в древние времена, она актуальна и на сегодняшний день. И, несомненно, наука будет актуальна и в будущем. Говорят, что если бы не было Баха, то мир никогда бы не услышал музыки. Но если бы не родился Эйнштейн, то теория относительности рано или поздно была бы открыта каким-нибудь ученым. Знаменитый афоризм Ф.Бэкона: «Знание - сила» сегодня актуален как никогда. Тем более, если в обозримом будущем человечество будет жить в условиях так называемого информационного общества, где главным фактором общественного развития станет производство и использование знания научно-технической и другой информации.

Таким образом, наука есть постижение мира, в котором мы живем. Соответственно науку принято определять как высокоорганизованную и высокоспециализированную деятельность по производству объективных знаний о мире, включающем и самого человека.

Вариант 6

Умные машины

Машины меняются. Домашние компьютеры нового типа пытаются вести себя как маленькие человечки. Чем думает машина? Не таким ли мозгом, как мы?

Увы, поведение этой старательной машины тоже пока далеко от разумного. Наш мозг легко отличает голос от посторонних шумов. Если за спиной собеседника хлопнет дверь, послышатся чьи-то шаги или зашелестит газета, мы пропустим эти негромкие звуки мимо ушей. Из беспорядочных звуков, долетающих до нас, а это миллион бит информации каждую секунду, мы выделяем лишь несколько сказанных нам слов. Мы равнодушны к шуршанию газетных листов и к хлопанью дверью. А вот ум компьютера подолгу сравнивает топот и звуки с любыми словами и не находит никакой разгадки услышанному. Компьютер готов сказать: «Смысл ваших слов невозможно понять». Человеческий мозг давно уже слышит лишь сказанное, и, более того, в век «информационной революции» мы невольно научились из целого ряда слов безошибочно улавливать только то, что относится к нам или к нашим интересам. Всю другую информацию мы умеем блокировать, мы защищаемся от нее. Это охраняет наш мозг и помогает нам в этом море сказанного и услышанного оставаться самим собой - личностью, а не

беспомощной машиной, с одинаковым интересом слушающей все вокруг и откликающейся на всякий звук, как компьютер.

Но и этого мало. Даже оказавшись в стерильных условиях, в изолированной комнате, один на один с человеком, машина по-прежнему теряется. Наша речь часто кажется ей бессмыслицей. В самых пустых разговорах мы по сто раз в день легко домысливаем сказанное. Где уж компьютеру, не знающему жизни, понять, что логику людям постоянно заменяют опыт и интуиция! Мы сразу угадываем намерение говорящего. Мы понимаем смысл сказанной фразы, не вдумываясь, как сочетаются ее части. В самых пустых разговорах мы по сто раз в день легко домысливаем сказанное. Компьютер не может этого делать. Чтобы научить компьютер думать так же, как мы, ученые предлагают пойти необычным путем.

Понятие «разум» предполагает, что, отталкиваясь от примитивного «дано», человек успевает молниеносно проделать сложнейшие мыслительные операции. Чтобы научить компьютер думать так же, как мы, ученые предлагают пойти необычным путем. «Разум состоит из десяти миллионов правил», - говорит американец Дуглас Ленат. Весь вопрос лишь в том, кто научит машину этим десяти миллионам правил, когда мы и сами затрудняемся назвать их. Бельгийский лингвист и компьютерщик Люк Стеелс считает, что с машинами нужно, как с детьми, играть в развивающие игры. Тогда машина сама усвоит правила, принятые в окружающем мире, и приспособится к ним. В его проекте «Talking heads» («Говорящие головы») участвует сразу несколько компьютеров. Они всматриваются в предметы, возникающие перед ними, указывают на них световым лучом и, совещаясь друг с другом, называют их соответствующими именами. Эти умные машины способны даже создавать целые предложения, пусть и очень простые.

Это радует ученых. Они давно мечтают о том, чтобы машины не только умели повторять заученные ими уроки, но и творили что-то новое, свое. Ведь человек, по образу и подобию, которого ученые начали создавать искусственные существа, постоянно все переделывает и создает свою собственную маленькую вселенную. (По материалам журнала «Знание – сила», 2000, № 9).

Вариант 7

Языки Ассемблер и Фортран, их классификация

Компьютер - автомат. И, в отличие от человека, работает только по программе, заложенной в него. Для написания таких программ в настоящее время применяются *алгоритмические языки программирования*, число которых уже превысило число языков человеческого общения. Но хотя разработаны тысячи языков программирования, лишь сотни из них реализованы хотя бы для одного компьютера, но и среди этих сотен языков активно используются лишь несколько десятков.

Существуют различные классификации языков программирования. Согласно одной из них, все языки программирования делятся на языки низкого уровня (машинно-ориентированные) и высокого уровня (символические).

Группу языков программирования *низкого уровня* обычно «открывает» язык *микрокоманд*. На основе простейшего набора микрокоманд пишутся специальные микропрограммы, определяющие, с одной стороны, элементарные операции компьютера, а с другой - управление выполнением программ из элементарных операций. Совокупность таких микропрограмм иногда называют *эмулятором*. Следующий по уровню язык из этой группы – *машинный*. Каждая его команда описывается последовательностью микрокоманд. Синтаксически эти команды не более, чем последовательности нулей и единиц. Машинный язык, как и язык микрокоманд, удобен для интерпретации аппаратурой компьютера, но плохо приспособлен для непосредственного использования человеком-программистом. Следующим в иерархии языков низкого уровня стоит обычно язык символического кодирования - АВТОКОД или АССЕМБЛЕР. Операторы этого языка - те же команды, но они имеют мнемонические (ассоциативные, буквенные) названия, а в качестве операндов используются не конкретные адреса в оперативной памяти, а их символические имена. Следующим естественным усложнением стала замена часто встречающихся последовательностей команд более крупными единицами - макрокомандами. Такие языки называют МАКРОЯЗЫКАМИ. Все языки низкого уровня ориентированы на определенный тип компьютера.

Следующую, существенно более многочисленную группу составляют языки программирования *высокого уровня*. Для всех языков высокого уровня общее то, что ориентированы они не на систему команд того или иного компьютера, а на систему операторов, характерных для записи определённого класса алгоритмов. Одним из первых языков высокого уровня был ФОРТРАН (Fortran). Уже само название его – ФОРмульный ТРАНслятор - говорит о том, что основное внимание здесь уделено удобному представлению формул. Уровень языка ФОРТРАН с позиций сегодняшнего дня не слишком высок, но он по-прежнему используется для инженерных и научных расчетов, и его популярность в значительной степени поддерживается физиками, усилиями которых созданы громадные библиотеки фортран-программ.

Таким образом, в процессе создания, реализации и использования языков фортран и ассемблер были отработаны многие важные идеи "языкотворчества" в программировании, и можно даже сказать, что эти языки дали уверенность в правильности самой концепции языков высокого уровня.

Вариант 8

Трансляторы

Все языки построены по определенным законам, в основе которых лежат алфавит и правила образования слов и предложений. Языки программирования строятся по тем же законам, что и человеческие: у них есть свой алфавит, свои слова (их еще называют служебными), свои правила написания. Программы, написанные на таких языках, состоят из последовательности предложений, которые называются *командами* или *операторами.* Двоим, говорящим на разных языках, для общения, наверное, понадобится человек, который знает эти оба языка. Он может помочь в разговоре, переводя с одного языка на другой. Если мы "заложим" в компьютер программу, написанную на одном из языков программирования, она не будет выполняться, компьютер ее не поймет. Сам компьютер понимает только один язык - язык машинных кодов (помните? Нули и единицы. Двоичное кодирование.) Чтобы программа была понята, ее надо перевести в машинный код. Для этого используются программы-переводчики, их называют *трансляторами* (от латинского translatio - "передача"). Трансляторы обычно подразделяют на два типа:

1) Компиляторы, переводящие целиком всю программу, написанную на языке программирования высокого уровня, на машинный язык, после чего программа записывается в память компьютера и лишь потом реализуется.

2) Интерпретаторы, переводящие команды или операторы входной программы по очереди и немедленно выполняющие их.

Любой транслятор решает четыре основные задачи:

1) Анализирует транслируемую программу, ищет ошибки, исправляет их сам или выдает сообщения об ошибках.

2) Если ошибок нет, транслятор генерирует выходную программу (ее часто называют объектной или рабочей) на машинном языке.

3) Оптимизирует (улучшает) выходную программу, действуя по двум основным направлениям: устранение недостатков программы, вызванных небрежностью или низкой квалификацией программиста, и сокращение излишних вычислений, неизбежно возникающих в процессе трансляции даже при самом тщательном написании программ на языке высокого уровня.

4) Распределяет машинную память для выходной программы.

Определить, что же такое хороший транслятор, довольно трудно. Известны очень быстро работающие трансляторы, дающие плохие программы; есть трансляторы, генерирующие чрезвычайно эффективные программы, но затрачивающие много времени на оптимизацию выходной программы. Большинство трансляторов - промежуточные между этими двумя типами.

Отсюда следует, что *система программирования* может включать в себя дополнительно к символическому языку программирования и

соответствующему транслятору текстовый редактор, библиотеки стандартных подпрограмм, отладчик компоновщик и другие сервисные средства.

Ведущими разработчиками систем программирования в настоящее время являются фирмы Microsoft и Borland International.

Вариант 9

Компоненты вычислительных сетей

Для определения компонентов вычислительных сетей приведем их общую классификацию. Для неё используются различные признаки, но чаще всего сети делят на типы по территориальному признаку, то есть по величине территории, которую покрывает сеть. И для этого есть веские причины, так как отличия технологий локальных и глобальных сетей очень значительны, несмотря на их постоянное сближение.

Делятся сети по степени территориальной распределенности на: глобальные (WAN), городские(MAN) и локальные(LAN).

К локальным сетям – Local Area Networks (LAN) – относят сети компьютеров, сосредоточенных на небольшой территории (обычно в радиусе не более 1-2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. Из-за коротких расстояний в локальных сетях имеется возможность использования относительно дорогих высококачественных линий связи, которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными. В связи с этим услуги, предоставляемые локальными сетями, отличаются широким разнообразием и обычно предусматривают реализацию в режиме on-line.

Глобальные сети – Wide Area Networks (WAN) – объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах. Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, в глобальных сетях часто используются уже существующие линии связи, изначально предназначенные совсем для других целей. Например, многие глобальные сети строятся на основе телефонных и телеграфных каналов общего назначения. Из-за низких скоростей таких линий связи в глобальных сетях (десятки килобит в секунду) набор предоставляемых услуг обычно ограничивается передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты.

Городские сети (или сети мегаполисов) – Metropolitan Area Networks (MAN) – являются менее распространенным типом сетей. Появились они сравнительно недавно и изначально предназначались для обслуживания территории крупного города – мегаполиса. В то время, как локальные сети наилучшим образом подходят для разделения ресурсов на коротких расстояниях и широковещательных передач, а глобальные сети обеспечивают работу на больших расстояниях, но с ограниченной скоростью и небогатым

набором услуг, сети мегаполисов занимают некоторое промежуточное положение. Они используют цифровые магистральные линии связи, часто – оптоволоконные, и предназначены для связи локальных сетей в масштабах города и соединения локальных сетей с глобальными. Эти сети первоначально были разработаны для передачи данных, но сейчас они поддерживают и такие услуги, как видеоконференции и интегральные передачи голоса и текста. Исторически сложилось так, что местные телефонные компании всегда обладали слабыми техническими возможностями и из-за этого не могли привлечь крупных клиентов. Сети мегаполисов являются общественными сетями, и поэтому их услуги обходятся дешевле, чем построение собственной (частной) сети в пределах города.

Таким образом, крупные сети практически никогда не строятся без логической структуризации. Для отдельных сегментов и подсетей характерны типовые однородные топологии базовых технологий, и для их объединения всегда используется оборудование, обеспечивающее локализацию трафика, - мосты, коммутаторы, маршрутизаторы и шлюзы.

Вариант 10

Разработка семантических электронных библиотек

В настоящее время имеется много разнородных электронных документов, доступных в компьютерных сетях. В связи с этим становится актуальной проблема организации работы с такими документами и содержащейся в них информацией, используя современные информационные технологии. Необходимо выполнять работу не столько с файлами, в которых содержатся документы, но и с их смыслом, содержащейся в них семантикой. Под электронными библиотеками понимаются информационные системы, которые автоматизируют решение основных проблем организации работы с документами. Уже достаточно давно предпринимались попытки разработки подходов к созданию электронных библиотек. Однако в связи с тем, что появляются новые требования и новые возможности, связанные с появлением новых технологий, необходимо разрабатывать и новые подходы к созданию ЭБ.

С появлением семантических технологий, позволяющих выполнять работу с семантикой документов, возникла возможность разработки новых подходов к автоматизации работы с электронными документами на новом уровне. В данной статье рассматриваются проблемы функционирования электронных библиотек, на основе которых разработана их модель, основанная на использовании семантических технологий.

Электронные библиотеки – это организации, в том числе специализированный персонал, представляющие доступ читателей к электронным ресурсам. Кроме того они выполняют отбор, структурирование, предоставление интеллектуального доступа, интерпретацию, распространение, сохранение целостности и обеспечение сохранности в

течение длительного времени наборов электронных документов для удобного доступа к ним определенным сообществам специалистов.

В соответствии с данным определением основными компонентами ЭБ являются: специалисты, информационные ресурсы (документы) и информационные технологии.

Электронные библиотеки реализуют набор функций для обеспечения читателям полного доступа к множеству распределенных и разнородных документов, содержащих информацию и знания, интегрируя их в единое информационное пространство.

Вот некоторые проблемы ЭБ, основными из которых являются следующие:

- проблема интеграции разнородной информации (электронных ресурсов, пользовательских профилей, таксономий) на основе различных метаданных, содержащих выразительные семантические описания;

- проблема поддержки взаимодействия с другими информационными системами (и не только ЭБ) либо с помощью метаданных, либо на уровне коммуникации или с помощью обеих возможностей. При этом в качестве единого языка взаимодействия между системами может использоваться язык RDF (Resource Description Framework);

- проблема обеспечения надежного, удобного и адаптируемого поиска и интерфейсов просмотра электронных документов, усиленных работой с семантикой.

Для решения таких проблем и улучшения функционирования ЭБ требуется разработать новый тип ЭБ на основе использования новых информационных технологий, в том числе семантических технологий. В этом случае такие ЭБ можно называть семантическими электронными библиотеками.

Вариант 11

Нанотехнологии в современных электронных системах

По своему назначению современные электронные системы охватывают широкую номенклатуру изделий, масштабы функционирования которых простираются от атомно-молекулярного уровня (нано- и микроструктуры) до планетного масштаба (телекоммуникации).

Разработка и производство разнообразных миниатюрных электронных систем является одним из стратегических направлений мирового научно-технического прогресса. Миниатюризация приводит к революционным изменениям техники, особенно в тех случаях, когда далеко не очевидным образом удается разработать и использовать технологию массового производства изделия, что позволяет существенно уменьшить го цену, повысить надежность, снизить энергопотребление и т.п. Эффективность миниатюризации наиболее ярко демонстрирует достижения микроэлектроники, компьютерной техники, телекоммуникации.

Для полувековой истории микроэлектроники характерны высокие темпы миниатюризации, которые описаны эмпирическими законами Мура в различных формулировках. Из наиболее распространенной формулировки следует, что плотность транзисторов в современных интегральных схемах удваивается каждые 18 месяцев. Однако в настоящее время ситуация в этой области качественно отличается от ситуации прошлого века.

В недалеком прошлом рекордные достижения миниатюризации при массовом производстве электронных систем характеризовалась пространственными масштабами в сотни и десятки микрон. Сейчас же рекордные достижения миниатюризации практически достигли нанометровых пространственных масштабов, т.е. элементарных физических объектов электроники.

Действительно, элементарными физическими объектами электроники являются атомы, состоящие из атомного ядра и электронов, и электромагнитное поле (фотоны). Типичные размеры атомов составляют десятые доли нанометра, а длина волны фотонов оптического диапазона электромагнитного сотни нанометров. Условно радиус электрона можно оценить величиной ~ 8*10^-6 нм.

Современные электронные системы имеют сложную иерархическую структуру, которые для своего функционирования реально интегрируют физико-химические явления от атомно-молекулярного уровня до макроскопического уровня. В архитектуре они неуклонно приближаются к архитектуре живых систем.

Вариант 12

Математическое моделирование технической системы

Математическую модель объекта можно представить в виде некоторого оператора, отображающего входные координаты объекта в выходные. В общем случае этот оператор может иметь вид алгебраических, дифференциальных, интегральных математических форм, являться непрерывным, принимать дискретные значения, быть кусочно-постоянным, логическим и т.п. Основной отличительной чертой математического моделирования является перевод моделируемых в объекте исследования процессов в другое временное пространство, где скорость протекания реальных процессов в объекте исследования соизмерима со скоростью решения математических форм (уравнений, неравенств, логических условий и т.п.), составляющих математическую модель объекта. Уход в другое временное пространство и, как следствие, получение значительного количества «свободного» времени, которое исследователь использует для анализа различных ситуаций по режимному и конструктивному оформлению протекания процессов в технической системе, является основным достоинством метода математического моделирования. Кроме этого, применение математического моделирования не требует материальных,

сырьевых, энергетических затрат, как это бывает при реализации (физическом моделировании) процессов в объекте исследования.

Здесь возникает ряд вопросов: если все так хорошо при реализации метода математического моделирования, почему этот метод применяется в полной мере не так уж часто, почему при его применении выявляется множество некорректных действий исследователя и почему результаты, получаемые с «благими» намерениями, зачастую являются ошибочными.

Выясняется следующая ситуация. Ответ на вышеперечисленные вопросы прост и однозначен – у исследователя нет необходимых для применения метода математического моделирования знаний (всех или части). Ситуация осложняется еще и тем, что глубина проработки кинетических закономерностей процессов в объекте исследования в конкретной прикладной области для конкретной постановки задачи может быть недостаточной или отсутствовать вообще.

В ряде других прикладных областей оценку технологических процессов, протекающих в объекте исследования, осуществляют на экспериментальных установках с фиксированными конструктивными характеристиками, которые в явной или неявной формах входят в кинетические уравнения. Естественно, что такие выражения сужают область определения разрабатываемой математической модели и должны четко отслеживаться исследователем.

Следует отметить, что процесс построения математической модели объекта исследования наиболее трудоемок и ответственен при исследовании и проектировании технических систем. Именно на этом этапе исследователем допускаются просчеты, которые могут существенно исказить искомые характеристики технической системы.

Вариант 13

Информация и вычислительные машины

Совершенно новые возможности для поиска и обработки информации открыло перед людьми изобретение в середине XX в. электронных вычислительных машин – ЭВМ (за рубежом эти машины получили название компьютер). Первоначально ЭВМ создавались для автоматизации вычислений. Затем их научили записывать и хранить информацию на магнитных лентах, печатать ее на бумаге, выводить на экран ЭВМ. По мере развития они стали использоваться для создания архивов, подготовки и редактирования текстов, выполнения чертежных и графических работ, автоматизации производства и многих других видов человеческой деятельности.

В 70-х годах развитие электроники послужило толчком для создания и массового производства нового вида компьютеров – персональных ЭВМ, которые сегодня широко применяются в школах, институтах, издательствах и т.п. Такие машины можно использовать для учебы, работы, игры и многих других целей. Применение таких ЭВМ на производстве, при проектировании,

в научных исследованиях и образовании может коренным образом изменить содержание деятельности и условия работы многих миллионов людей. Прежде всего, ЭВМ открывают возможности для создания автоматизированных технологий производства. С их помощью можно создавать новые виды машин, приборов и устройств, управляемых с помощью ЭВМ.

К началу XXI вычислительные машины на базе таких устройств сделали возможным создание «безлюдных» технологий производства. На таких «фабриках будущего» физическая работа будет выполняться роботами, а роль людей сведется к планированию производства, программированию роботов и проектированию новых изделий с помощью ЭВМ. Применение ЭВМ во многих видах деятельности уже сейчас позволяет существенно упростить работу людей по подготовке, накоплению и переработке информации, проведению проектно-конструкторских работ и научных исследований. Электронно-вычислительные машины уже есть в школах и они будут помогать при изучении физики и математики, химии, биологии и многих других учебных предметов.

Умение общаться с ЭВМ и использовать их в своей работе, так же, как умение пользоваться ручкой, в ближайшие 10-15 лет, станет необходимым практически для всех и составит основу компьютерной грамотности. Компьютерная грамотность – это умение читать и писать, считать и рисовать, а также искать информацию, применяя для этого ЭВМ. Умение эффективно использовать ЭВМ в работе предполагает определенную культуру. Она включает в себя знание основных возможностей ЭВМ: умение четко ставить задачи, составлять планы их решения и записывать их в форме, понятной ЭВМ; умение выделять данные для решения задач и анализировать получаемые результаты. Эта культура опирается на знание законов логики и информатики.

Вариант 14

ЭВМ

На протяжении всей истории своего развития человечество испытывало потребность в проведении расчетов. На первом этапе ему хватало самых простейших устройств, например, пальцев рук или ног. С развитием науки и техники возрастала необходимость в расчетах, и для их облегчения были разработаны специальные устройства - абак, счеты, арифмометры, специальные математические таблицы. Однако уже к середине 40-х годов, особенно в связи с развитием ядерной физики, расчеты, проводимые вручную человеком, требовали больших материальных и людских ресурсов. Например, при работе над «Манхэттенским проектом» (разработка атомной бомбы в США) было привлечено более 600 человек, часть из которых проводила расчеты, а другая – занималась проверкой правильности их вычислений.

Потребность в автоматизации обработки информации в середине XX века (в том числе для военных нужд) привела к бурному развитию электронной техники и технологии.

Созданные на базе достижений электроники технические устройства стали называть электронно-вычислительными машинами (ЭВМ).

Вычислительные машины представляют собой новое качество в сравнении со всеми устройствами, которые были прежде изобретены человеком. Они увеличивают не физическую силу человека, они увеличивают возможности его интеллекта.

Пока электронно-вычислительные машины делают первые шаги. Они только считают, производят простейшие логические операции. Они остаются еще совершенно безвольными, выполняя лишь то, что человек им покажет. И все-таки уже сейчас ясно: в принципе этим машинам человек может поручить любую интеллектуальную работу. Больше того, можно создать и такие машины, у которых будут «собственные чувства».

Простейшие чувства – это физические ощущения. Машина может воспринимать их дифференцированно. Машина, снабженная всевозможными акустическими, оптическими, тепловыми приборами (аналогами наших органов чувств), может воспринимать окружающую обстановку и оценивать ее. Но, конечно, при условии, что конструктор наделит ее такими свойствами – введет в схему машины соответствующие устройства, или введет «программу реагирования».

Вопрос восприятия можно уже считать технически решенным. Сейчас многие математики и кибернетики занимаются проблемой распознавания образов машиной. Машина сама должна определить, какие именно образы она восприняла. Есть машины, которые распознают печатный текст, буквы, звуки. Можно сделать так, что эти воспринятые и расшифрованные машиной образы будут связаны в ней определенными «эмоциями».

В зависимости от характера восприятий и их оценки машина предпримет те или иные действия. Можно заложить в нее и волю — задать в программе определенную цель существования машины. Так машина по всем признакам может стать моделью мыслящего существа. (По статье Д. Усенкова, «Знание – сила», 2000, №2)

Вариант 15

Технология клиент-сервер

Характер взаимодействия компьютеров в локальной сети принято связывать с их функциональным назначением. Как и в случае прямого соединения, в рамках локальных сетей используется понятие клиент и сервер. Технология клиент-сервер — это особый способ взаимодействия компьютеров в локальной сети, при котором один из компьютеров (сервер) предоставляет свои ресурсы другому компьютеру (клиенту). В соответствии с этим различают одноранговые сети и серверные сети.

При одноранговой архитектуре в сети отсутствуют выделенные серверы, каждая рабочая станция может выполнять функции клиента и сервера. В этом случае рабочая станция выделяет часть своих ресурсов в общее пользование всем рабочим станциям сети. Как правило, одноранговые сети создаются на базе одинаковых по мощности компьютеров. В том случае, когда сеть состоит из небольшого числа компьютеров и ее основной функцией является обмен информацией между рабочими станциями, одноранговая архитектура является наиболее приемлемым решением. Подобная сеть может быть достаточно быстро и просто реализована средствами такой популярной операционной системы как Windows 98.

Наличие распределенных данных и возможность изменения своих серверных ресурсов каждой рабочей станцией усложняет защиту информации от несанкционированного доступа, что является одним из недостатков одноранговых сетей. Другим недостатком одноранговых сетей является их более низкая производительность. Это объясняется тем, что сетевые ресурсы сосредоточены на рабочих станциях, которым приходится одновременно выполнять функции клиентов и серверов.

В серверных сетях осуществляется четкое разделение функций между компьютерами: одни их них постоянно являются клиентами, а другие - серверами. Учитывая многообразие услуг, предоставляемых компьютерными сетями, существует несколько типов серверов, а именно: сетевой сервер, файловый сервер, сервер печати, почтовый сервер и др.

Сетевой сервер представляет собой специализированный компьютер, ориентированный на выполнение основного объема вычислительных работ и функций по управлению компьютерной сетью. При подобной сетевой организации функции рабочих станций сводятся к вводу-выводу информации и обмену ею с сетевым сервером.

Термин *файловый сервер* относится к компьютеру, основной функцией которого является хранение, управление и передача файлов данных. Он не обрабатывает и не изменяет сохраняемые и передаваемые им файлы. Сервер может «не знать», является ли файл текстовым документом, графическим изображением или электронной таблицей. В общем случае на файловом сервере может даже отсутствовать клавиатура и монитор. Все изменения в файлах данных осуществляются с клиентских рабочих станций. Для этого клиенты считывают файлы данных с файлового сервера, осуществляют необходимые изменения данных и возвращают их обратно на файловый сервер. Подобная организация наиболее эффективна при работе большого количества пользователей с общей базой данных. В рамках больших сетей может одновременно использоваться несколько файловых серверов.

Вариант 16

Прорывы в неведомое

Человеческий мозг нельзя сравнивать с компьютером, прибегая к такой логике: «Мозг обрабатывает информацию, и микросхемы обрабатывают информацию. Значит, мозг похож на микросхему». Обрабатывать информацию можно по-разному. Машина делает, например, все операции последовательно, мы – параллельно - последовательно. По ассоциации мы выхватываем из глубин памяти сведения, много лет назад отложенные и, наконец, пригодившиеся. Мозг машины может на 90 процентов работать, как человеческий. Но остальные 10 процентов – это творческий интеллект. Его никак не воспроизвести.

Американец Джон Сирл сравнивает поведение компьютера с действиями человека. Выучив правила китайской грамоты и иероглифы, компьютер может складывать из них слова, но что означает этот набор знаков, для него по-прежнему непонятно. Философ делает вывод: даже если появятся машины, которые, будучи соответствующим образом запрограммированы, станут вести себя, как человек, наделенный разумом, это не доказывает, что разум у них есть. А способна ли неразумная машина, как бы сильна она ни была, справиться с человеком? Ее сила будет всегда применяться по определенной схеме. Человек же, наделенный хоть искрой творческого духа, всегда играет не по правилам. Каждый человек – сам по себе – уникален. Каждый нормальный человек думает (и порой поступает) «не как все».

Вовсе несложно сконструировать лет через сто аппараты, которые поведут себя вроде бы так же, как мы. Они будут осязать, осматривать окружающий их мир, прислушиваться к нему, сканировать книги и газеты, складывая в своем электронном мозгу миллиарды и миллиарды строчек. Но ощущения, вызываемые предметами и событиями, – это больше, чем реакция на них: «Препятствие – уклониться», «Съедобное – съесть», «Горячее – избежать». Нет, ощущения иногда навсегда остаются в нашем сознании и вызывают совсем иные эмоции, воспоминания... Например, огонь неожиданно заставляет вспомнить давний зимний праздник на даче.

Конечно, машины могут очень затруднить жизнь человека. Простая размагниченная дискета порой перечеркивает не один месяц ваших трудов. Обесточенные приборы в городах, где иногда отключают электричество, сразу превращают горожанина в инвалида, не способного ни приготовить пищу, ни узнать о происходящем вокруг.

И все-таки человек – не машина, моментально прекращающая работать, если «пункт А не выполнен». Человек способен выбраться из любых трудных ситуаций, привыкнуть к любым условиям. И даже если машины восстанут, человек найдет выход из этого положения.

За любым прорывом в неведомое, за любой революцией – социальной и научной – следует мощный откат. Оптимизм слеп и обманчив. Триумф науки и искусства начала века сменился общеевропейским «тоталитарным

рабством» 1930-1940-х годов. Чем обернется новый научный взлет 1980-1990-х годов? И машины ли станут причиной будущих бед? Да и вообще – превзойдут ли машины человека? (По статье Александра Грудинкина, «Знание – сила», 2000, № 9).

Вариант 17

Языки Паскаль и Бейсик

Алгоритмический язык ПАСКАЛЬ (Pascal) разработан в 1970 г. Норбертом Винером и назван в честь английского учёного Б. Паскаля. По своей идее это алголоподобный язык, вобравший в себя все лучшие проектные решения предшественника. Но вместе с тем это качественно новый шаг, связанный прежде всего с тем, что здесь впервые была воплощена концепция абстрактных типов данных. Почти одновременно с паскалем, в начале 70-х годов, был разработан и язык программирования СИ (С). Но если паскаль шел больше от теории программирования, то язык СИ - типичный пример влияния практических потребностей системного программирования на разработку новых языков. Изначально он создавался как инструментальное средство для реализации операционной системы UNIX на компьютеры фирмы DEC, но популярность его быстро переросла рамки конкретной машины, и сейчас язык СИ можно по праву назвать одним из универсальных языков программирования. В добавление к средствам языка паскаль в СИ включены средства программирования почти на уровне ассемблера.

Язык БЕЙСИК (Basic), изучением которого мы с вами будем теперь заниматься, был разработан в 1964 году в США сотрудниками Дармутского колледжа Джоном Кемени и Томасом Курцем. Название языка образовано начальными буквами предложения Beginners All-purpose Simbolic Instruction Code, что в переводе означает - Многоцелевой Символический Код для начинающих. Интересно отметить, что язык под названием Бейсик существовал задолго до появления компьютеров. Он состоял примерно из 300 английских слов и использовался в Африке местными жителями для общения с английскими миссионерами и как язык межплеменного общения. Отношение к Бейсику среди профессионалов весьма противоречивое. Одни вообще не считают его заслуживающим внимания (например, в энциклопедическом словаре ИНФОРМАТИКА для начинающих такого слова просто нет). А известный специалист в области информатики Р.Форсайт писал: «БЕЙСИК - это питон, пожирающий все на своем пути. БЕЙСИК только что закончил «переваривать» язык ПАСКАЛЬ со всеми его управляющими структурами. После небольшой паузы и нескольких отрыжек он будет в состоянии «слопать» ПРОЛОГ..». Языки логического программирования ЛИСП (1959 г.), ПРОЛОГ (1973 г.), РЕФАЛ предназначены для обработки не столько числовой, сколько символьной информации. Центральным понятием в логическом программировании

является отношение. Программа представляет собой совокупность определений отношений между объектами и цели.

Вариант 18

Прерывания

Прерывания представляют собой механизм, позволяющий координировать параллельное функционирование отдельных устройств вычислительной системы и реагировать на особые состояния, возникающие при работе процессора, т.е. – это принудительная передача управления от выполняемой программы к системе (а через нее – к соответствующей программе обработки прерывания), происходящая при возникновении определенного события. Основная цель введения прерываний – реализация асинхронного режима функционирования и распараллеливание работы отдельных устройств вычислительного комплекса. Механизм прерываний реализуется аппаратно-программными средствами.

Механизм обработки прерываний независимо от архитектуры вычислительной системы подразумевает выполнение некоторой последовательности действий:

- *шаг 1*: установление факта прерывания (прием сигнала запроса на прерывание) и идентификация прерывания;
- *шаг 2*: запоминание состояния прерванного процесса вычислений. Состояние процесса выполнения программы определяется значением счетчика команд, содержимым регистров процессора, а также может содержать спецификацию режима и другую информацию;
- *шаг 3*: управление аппаратно передается на подпрограмму обработки прерывания. В простейшем случае в счетчик команд заносится начальный адрес подпрограммы обработки прерываний, а в соответствующие регистры – информация из слова состояния;
- *шаг 4*: сохранение информации о прерванной программе, которую не удалось спасти (на шаге 2) с помощью аппаратуры;
- *шаг 5*: собственно выполнение программы, связанной с обработкой прерывания. Эта работа может быть выполнена той же подпрограммой, на которую было передано управление на шаге 3, но в ОС достаточно часто она реализуется путем последующего вызова соответствующей подпрограммы;
- *шаг 6*: восстановление информации, относящейся к прерванному процессу (этап, обратный шагу 4);
- *шаг 7*: возврат в прерванную программу.

Шаги 1-3 реализуются аппаратно, шаги 4-7 – программно.

Главные функции механизма прерываний:

- распознавание или классификация прерываний;
- передача управления соответствующему обработчику прерываний;
- корректное возвращение к прерванной программе.

Переход от прерываемой программы к обработчику и обратно должен выполняться как можно быстрей. Одним из самых простых и быстрых методов является использование таблицы, содержащей перечень всех допустимых прерываний и адреса соответствующих обработчиков. Для корректного возвращения к прерванной программе перед передачей управления обработчику прерываний содержимое регистров процессора запоминается либо в памяти с прямым доступом, либо в *системном стеке* (system stack).

Прерывания, возникающие при работе вычислительной системы, можно разделить на два основных класса: *внешние* (*асинхронные*) и *внутренние* (*синхронные*).

Вариант 19

Вычислительный процесс и ресурсы

Последовательный процесс (*задача – task*) – это отдельная программа с ее данными, выполняющаяся на последовательном процессоре (т.е. таком процессоре, в котором текущая команда выполняется после завершения предыдущей).

В современных процессорах для повышения скорости вычислений возможно параллельное выполнение нескольких команд, что достигается двумя основными способами – *организацией конвейерного механизма выполнения команды* и *созданием нескольких конвейеров*. Однако в подобных процессорах обязательно достигается логическая последовательность в выполнении команд, предусмотренная программой.

Концепция процесса предполагает два аспекта:

- процесс является носителем данных;
- процесс выполняет задачи, связанные с обработкой данных.

В качестве примеров процессов (задач) можно назвать прикладные программы пользователей, утилиты и другие системные обрабатывающие программы. Процессом может быть редактирование текста, трансляция исходной программы, ее компоновка, исполнение. Трансляция какой-нибудь исходной программы является одним процессом, а трансляция следующей исходной программы – другим, т.к. транслятор выступает как одна и та же программа, но обрабатываемые данные являются разными. Основная цель процесса - выработать механизмы распределения и управления ресурсами.

Ресурсы – это многократно используемые, относительно стабильные и часто недостающие объекты, которые запрашиваются, задействуются или освобождаются в период их активности, т.е. всякий объект, который может распределяться внутри системы. Ресурсы могут быть *разделяемыми*, когда несколько процессов используют их *одновременно* или *параллельно* (попеременно в течение некоторого интервала времени), и *неделимыми* (рисунок 1).

В настоящее время понятие ресурса – это абстрактная структура с целым рядом атрибутов, характеризующих способы доступа к этой структуре и ее физическое представление в системе (системные ресурсы), а также такие объекты, как сообщения и синхросигналы, которыми обмениваются задачи.

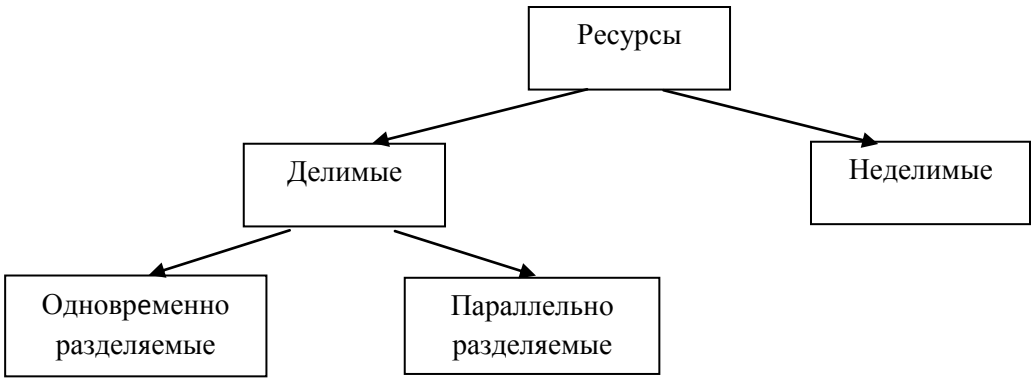

Рисунок 1 – Классификация ресурсов

В первых вычислительных системах любая программа могла выполняться только после полного завершения предыдущей. Поскольку все эти системы были построены в соответствии с принципами фон Неймана, все подсистемы и устройства компьютера управлялись исключительно центральным процессором. Соответственно, пока осуществлялся обмен данными между оперативной памятью и внешними устройствами, процессор не мог выполнять вычисления. Введение в состав вычислительной машины специальных контроллеров позволило *совместить во времени* (*распараллелить*) операции вывода полученных данных и последующие вычисления на центральном процессоре. Однако все равно процессор часто и долго простаивал, дожидаясь завершения очередной операции ввода-вывода. Поэтому возникла необходимость в организации *мультипрограммного* (*мультизадачного*) режима работы.

Итак, ОС может поддерживать мультипрограммирование (многопроцессорность). В этом случае необходимо эффективно использовать имеющиеся ресурсы путем организации к ним очередей запросов. Это требование достигается поддерживанием в памяти более одного вычислительного процесса, ожидающего процессор, и более одного процесса, готового использовать другие ресурсы, как только они станут доступными.

Вариант 20

Дисциплина диспетчеризации FCFS

Дисциплины диспетчеризации (*обслуживания*) – это правила формирования очереди готовых к выполнению задач, в соответствии с которыми формируется эта очередь (список). Различают два больших класса дисциплин обслуживания: *бесприоритетные* и *приоритетные*. При

бесприоритетном обслуживании выбор задач производится в некотором заранее установленном порядке без учета их относительной важности и времени обслуживания. При реализации приоритетных дисциплин обслуживания отдельным задачам предоставляется преимущественное право попасть в состояние исполнения. В концепции приоритетов имеются следующие варианты: приоритет, присвоенный задаче, является величиной постоянной; приоритет изменяется в течение времени решения задачи (динамический приоритет).

Диспетчеризация с динамическими приоритетами требует дополнительных расходов на вычисление значений приоритетов исполняющихся задач, поэтому во многих ОС реального времени используются методы диспетчеризации на основе абсолютных приоритетов. Это позволяет сократить время реакции системы на очередное событие, однако требует детального анализа всей системы для правильного присвоения соответствующих приоритетов всем исполняющимся задачам, чтобы гарантировать обслуживание.

Самой простой в реализации является *дисциплина FCFS* (First Come First Served – первый пришел, первым обслужен), согласно которой задачи обслуживаются «в порядке очереди», т.е. в порядке их появления. Те задачи, которые были заблокированы в процессе работы (попали в состояние ожидания, например из-за операций ввода-вывода) после перехода в состояние готовности вновь ставятся в эту очередь готовности. При этом возможны два варианта:

1) ставить разблокированную задачу в конец очереди готовых к выполнению задач (самый простой, применяется чаще всего);

2) диспетчер помещает разблокированную задачу перед теми задачами, которые еще не выполнялись – т.е. образуется две очереди: одна из новых задач, а другая – из ранее выполнявшихся задач, попавших в состояние ожидания.

Таким образом, дисциплина не требует внешнего вмешательства в ход вычислений, при ней не происходит перераспределения процессорного времени. Она относится к не вытесняющим дисциплинам. Достоинства: простота реализации и малые расходы системных ресурсов на формирование очереди задач. Недостаток: при увеличении загрузки вычислительной системы растет среднее время ожидания обслуживания, причем короткие задания вынуждены ожидать столько же, сколько и трудоемкие. Избежать этого недостатка позволяют дисциплины SJN и SRT.

Вариант 21

Помехоустойчивое кодирование

Бурный рост теории и практики помехоустойчивого кодирования в последнее десятилетие связан, в первую очередь, с созданием средств телеобработки данных, вычислительных систем и сетей, региональных

автоматизированных систем управления, систем автоматизации научных исследований. Высокие требования к достоверности передачи, обработки и хранения информации в указанных системах диктовали необходимость такого кодирования информации, которое обеспечивало бы возможность обнаружения и исправления ошибки.

Коды, обладающие свойствами обнаружения и исправления ошибок, называют помехоустойчивыми. Они используются как для исправления ошибок (корректирующие коды), так и для их обнаружения.

Классификация помехоустойчивых кодов. У подавляющего большинства существующих в настоящее время помехоустойчивых кодов указанные условия являются следствием их алгебраической структуры. В связи с этим их называют алгебраическими кодами. (В отличие, например, от кодов Вагнера, корректирующее действие которых базируется на оценке вероятности искажения каждого символа).

Алгебраические коды можно подразделить на два больших класса: *блоковые и непрерывные*.

В случае *блоковых кодов* процедура кодирования заключается в сопоставлении каждой букве сообщения (или последовательности из k символов, соответствующей этой букве) блока из n символов. В операциях по преобразованию принимают участие только указанные k символов, и выходная последовательность не зависит от других символов в передаваемом сообщении.

Блоковый код называют равномерным, если n остается постоянным для всех букв сообщения.

Различают разделимые и неразделимые блоковые коды. При кодировании разделимыми кодами выходные последовательности состоят из символов, роль которых может быть отчетливо разграничена. Это информационные символы, совпадающие с символами последовательности, поступающей на вход кодера канала, и избыточные (проверочные) символы, вводимые в исходную последовательность кодером канала служат для обнаружения и исправления ошибок.

При кодировании неразделимыми кодами разделить символы выходной последовательности на информационные и проверочные невозможно.

Непрерывными (древовидными) называют такие коды, в которых введение избыточных символов в кодируемую последовательность информационных символов осуществляется непрерывно, без разделения ее на независимые блоки. Непрерывные коды также могут быть разделимыми и неразделимыми.

Наиболее простыми в отношении технической реализации кодами этого класса являются сверточные (рекуррентные) коды.

Вариант 22

Управляемые и неуправляемые динамические системы

Первые шаги, положившие начало развитию системного анализа, были сделаны античными астрономами. Их роль была пассивной: наблюдать. В аналогичном положении находятся современные исследователи, работающие, например, в области астрофизики. Они пока еще также вынуждены ограничиться только наблюдениями каких-то процессов, не имея возможности ими управлять.

В то же время современный исследователь призван играть активную роль в развитии наблюдаемого процесса, поскольку именно он генерирует соответствующие внешние воздействия, гарантирующие удовлетворительное поведение системы. Разумеется, при таком подходе активного вмешательства возникает множество проблем психологического и морального характера. Подобное разделение на активную и пассивную или управляемую и неуправляемую динамику позволяет наиболее наглядно выявить отличие классического и современного взглядов на системный анализ.

Ограничения

Системный анализ, как и политика, — это прежде всего искусство действовать в пределах «возможного». Рассматривая математическую формулировку той или иной задачи, исследователь (или лицо, принимающее решение) должен полностью представлять себе те внутренние и внешние факторы, которые могут ограничить его выбор стратегий управления. Различные обстоятельства, связанные с объемом имеющихся ресурсов, способом, который необходимо удовлетворить имеющейся технологией, наличием и возможностями ЭВМ, людскими ресурсами, бюджетом времени и т.д., резко сужают круг возможностей, доступных исследователю.

Выделим два принципиально различных типа ограничений:

1) Внутренние — ограничения, налагаемые структурой самой системы.

2) Внешние — ограничения, налагаемые на поведение системы внешними факторами.

Оптимизация

Одна из наиболее злободневных проблем анализа систем, рассматриваемых в социально-экономических задачах, — это проблема выбора критерия, т.е. вопрос о том, каким образом следует сравнивать между собой различные реализации поведения систем. К счастью, динамические процессы, наблюдаемые в физических и биологических системах, часто протекают по вполне определенным законам, которые, как правило, являются следствием различных принципов минимума или законами сохранения. Однако перенос этих законов на объекты социальной природы в лучшем случае носит искусственных характер и, более того, часто просто невозможен.

Важно отметить, что, хотя динамика системы остается неизменной, выбор иного критерия приводит к качественному изменению оптимального управления.

Вариант 23

Состояние проблемы и перспективы системных исследований

Системы автоматизации (СА) – это новое научное направление интеграционного типа, которое разрабатывает системную методологию принятия решений в процессе создания и развития сложных технических систем. В частности, автоматизированная система управления (АСУ) различных уровней и назначения. Характерно, что системный анализ выступает в одной связке с математическим моделированием и системным проектированием, т.к. анализ решений требует их модельной проработки, а проектирование есть основная сфера применения СА. Кроме того, СА опирается на достижения современной информатики, вычислительной техники и автоматизации.

В рамках системного анализа развивается теория принятия решений при многих критериях, которая приобретает статус научной подкладки в задачах прогнозирования, планирования, проектирования и управления. При этом особую важность имеет разработка прикладных инженерных методик, реализующих методологию системного анализа и позволяющих учесть многовариантность, многокритериальность, разнообразие внешней среды, неопределенность и риск.

Проблемы в области системного анализа связаны с разработкой научного инструментария для принятия решений. В частности, для инженерной практики, необходимы следующие методы:

- методы структуризации исследуемых объектов;
- методы декомпозиции и композиции;
- методы получения экспертной информации;
- методы многоцелевого математического программирования (40 на новом уровне);
- методы дискретной многокритериальной оптимизации;
- методы генерации альтернативных решений;
- методы отбраковки неперспективных решений;
- методы идентификации предпочтения ЛПР;
- методы психологического обоснования решений и др.

Перспективы в области СА связаны с:

- дальнейшим развитием концептуального и математического аппарата;
- автоматизацией процессов принятия решений на основе новой информационной технологии решения задач.

Автоматизации подлежат процессы принятия решений в АСУП, АСНИ, САПР, АСТПП, ГАП, АСКИ (комплексных испытаний) и др. системах.

Особое место занимает АСППР, которые создаются специально для усиления интеллекта ППР в задачах принятия решений.

Вариант 24

Назначение и общие принципы организации АСУТП

Автоматизированные системы управления технологическими процессами (АСУТП) – человеко-машинная система, в которой человек принимает содержательное участие в выработке решения.

АСУТП осуществляет воздействие на объект в том же, что и протекающие в нем процессы, т.е. АСУТП работает в режиме реального времени. В АСУТП в качестве объекта выступает ТОУ (технологический объект управления).

ТОУ представляет собой совокупность технологического оборудования и реализуемого на нем по соответствующим инструкциям и регламентам технологического процесса производства целевого продукта. В качестве ТОУ в АСУТП рассматриваются технологические установки, отдельные производства и технологические процессы всего предприятия.

При создании АСУТП необходимо определить цель этой системы.

Степень достижения поставленной цели принято характеризовать с помощью критериев управления.

Критерий управления должен быть обязательно выражен количественно и зависеть от выбранных управляющих воздействий.

Виды подсистем:

АСУТП реализует свои функции с помощью следующих подсистем.

1) Сбор и первичная обработка информации:
- сбор информации с ТОУ;
- проверка достоверности информации;
- фильтрация сигналов измерительной информации;
- расчет действительных значений параметров;
- усреднение и интегрирование значений параметров.

2) Контроль состояния объекта:
- отображение информации ;
- контроль и регистрация отклонения параметров от заданных значений;
- анализ срабатывания блокировок и защит.

3) Автоматическое регулирование и оптимальное управление:
- стабилизация технологических параметров;
- каскадное и связанное регулирование;
- логическое управление;
- дискретное, программное управление задвижками;
- статическая оптимизация.

4) Расчет технико-экономических показателей:
- расчет себестоимости продукции;
- расчет материального баланса.

5) Связь с MES – системой (АСУ предприятия):
- передача сообщений на верхний уровень;
- прием сообщений с верхнего уровня.

Вариант 25

Системы реального времени

Real-time system система реального времени (СРВ) – это любая система, в которой существенную роль играет время генерации выходного сигнала. Это обычно связано с тем, что входной сигнал соответствует каким-то изменениям в физическом процессе, и выходной сигнал должен быть связан с этими же изменениями. Временная задержка от получения входного сигнала до выдачи выходного сигнала должна быть небольшой, чтобы обеспечить приемлемое время реакции. Время реакции является системной характеристикой: при управлении ракетой требуется реакция в течении нескольких миллисекунд, тогда как для диспетчерского управления движением пароходов требуется время реакции, измеряемое днями.

Системы обычно считаются системами реального времени, если время их реакции имеет порядок миллисекунд; диалоговыми считаются системы с временем реакции порядка нескольких секунд, а в системах пакетной обработки время реакции измеряется часами или днями. Примерами систем реального времени являются системы управления физическими процессами с применением вычислительных машин, системы торговых автоматов, автоматизированные системы контроля и автоматизированные испытательные комплексы.

Режим реального времени [*real time processing*].

Режим обработки данных, при котором обеспечивается взаимодействие вычислительной системы с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов.

Пример – цикл управления самолетом, летящим на автопилоте. Датчики самолета должны постоянно передавать измеренные данные в управляющий компьютер. Если данные измерений теряются, то качество управления самолетом падает, возможно вместе с самолетом.

Пример – выделение самостоятельных программно-технических комплексов с функциями сбора, первичной обработки и передачи информации (PI System). PI System предоставляет информацию о технологических процессах в реальном масштабе времени на уровень управления производством и бизнес-систем для специалистов среднего и верхнего звеньев предприятия.

PI System - это инструмент построения информационной системы производства реального времени для промышленного предприятия. PI System наилучшим образом обеспечивает сбор, хранение и представление в едином формате данных от различных SCADA-систем, DCS, ПЛК, устройств ручного ввода, заводских лабораторий и т.п.

Тексты для выполнения СРС № 2 и № 3 специальности 5В100200 – Системы информационной безопасности

Вариант 1

Методы защиты информации

Джэймс Мэсси доказал, что после шести раундов шифрования алгоритмом обеспечивается абсолютная устойчивость к дифференциальному криптоанализу. При этом уже после трёх раундов шифрования линейный криптоанализ также становится неэффективным для взлома.

Несмотря на это, в 1995 году Ларсом Кнудсеном была обнаружена слабость в алгоритме генерации ключей для быстрой процедуры шифрования SAFER K-64. Он показал, что для любого ключа шифрования K1 можно найти один или несколько (вплоть до девяти) ключей K2 (отличающихся от него значением лишь одного байта) таких, что при зашифровании двух различных исходных текстов M1 и M2 получается один и тот же шифротекст, что можно записать в виде E(M1,K1) = E(M2,K2). Число различных открытых текстов M, из которых получается один и тот же шифротекст, лежит в промежутке между 222 и 228 из возможных 264 текстов. Таким образом, путём анализа от 244 до 247 открытых текстов можно вычислить 8 бит секретного ключа длиной 64-бита. Эта атака в дальнейшем была значительно усилена Джоном Келси (англ. John Kelsey), Брюсом Шнайером и Дэвидом Вагнером (англ.) (англ. David A. Wagner). Авторы атаки утверждали, что алгоритм легко поддаётся атакам на связанных ключах за счёт очень простой и однообразной процедуры генерации подключей.

Это свойство значительно уменьшает надёжность алгоритма при использовании его в качестве однонаправленной хэш-функции. Его надёжность как алгоритма шифрования при этом не уменьшается. Тем не менее, эта слабость алгоритма, вместе с атакой, в дальнейшем опубликованной Мёрфи, побудили Мэсси улучшить алгоритм генерации ключей. В результате в сентябре 1995 года им был опубликован алгоритм.

Французский криптограф Серж Водено (англ.) (фр. Serge Vaudenay) показал, что при замене содержимого S-блоков случайными перестановками, алгоритм становится менее криптостойким.

Таким образом, злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале

несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информации.

Вариант 2

Критерии и классы защищенности средств вычислительной техники

Блочный шифр – разновидность симметричного шифра. Особенностью блочного шифра является обработка блока нескольких байт за одну итерацию (как правило, 8 или 16). Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа.

Преобразование должно использовать следующие принципы:

1) Рассеивание (diffusion), то есть изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста.

2) Перемешивание (confusion) – использование преобразований, затрудняющих получение статистических зависимостей между шифротектстом и открытым текстом.

К достоинствам блочных шифров относят похожесть процедур шифрования и расшифрования, которые, как правило, отличаются лишь порядком действий. Это упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и дешифрования.

Основная идея

Блочный шифр состоит из двух взаимосвязанных алгоритмов: алгоритм шифрования E и алгоритм расшифрования E-1. Входными данными служат блок размером n бит и k-битный ключ. На выходе получается n-битный зашифрованный блок. Для любого фиксированного ключа функция расшифрования является обратной к функции шифрования для любого блока M и ключа K.

Для любого ключа K, EK является биективной функцией (перестановкой) на множестве n-битных блоков.

Размер блока n – это фиксированный параметр блочного шифра, обычно равный 64 или 128 битам, хотя некоторые шифры допускают несколько различных значений. Длина 64 бита была приемлема до середины 90-х годов, затем использовалась длина 128 бит, что примерно соответствует размеру машинного слова и позволяет эффективную реализацию на большинстве распространённых вычислительных платформах. Различные схемы шифрования позволяют зашифровывать открытый текст произвольной длины. Каждая имеет определенные характеристики: вероятность ошибки, простота доступа, уязвимость к атакам. Типичными размерами ключа являются 40, 56, 64, 80, 128, 192 и 256 бит. В 2006 г. 80-битный ключ способен был предотвратить атаку грубой силой.

Вариант 3

Основные функции подсистемы защиты операционной системы

Подсистема защиты операционной системы (ОС) выполняет следующие основные функции:

1) Идентификация и аутентификация. Ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2) Разграничение доступа. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

3) Аудит. ОС регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4) Управление политикой безопасности. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в ОС.

5) Криптографические функции. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6) Сетевые функции. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе и задач, имеющих прямое отношение к защите информации.

Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями под системы защиты должен существовать четко определенный интерфейс, используемый при взаимодействии модулей для решения общих задач.

В таких ОС, как Windows XP, подсистема защиты четко выделяется в общей архитектуре ОС, в других, как UNIX, защитные функции распределены практически по всем элементам ОС. Однако любая ОС, удовлетворяющая стандарту защищенности, должна содержать подсистему защиты, выполняющую все выше перечисленные функции. Обычно подсистема защиты ОС до пускает расширение дополнительными программными модулями.

Вариант 4

Особенности разработки сложных программных систем

Большинство современных программных систем являются достаточно сложными. Эта сложность обуславливается многими причинами, главной из которых является *логическая сложность* решаемых ими задач.

Раньше компьютеры применяли в очень узких областях науки и техники, в первую очередь там, где задачи были хорошо детерминированы и требовали значительных вычислений. Сейчас, когда созданы мощные компьютерные сети, появилась возможность переложить на них решение сложных ресурсоемких задач, о компьютеризации которых раньше не задумывались.

Подавляющее большинство сложных систем имеет *иерархическую* внутреннюю структуру. Связи элементов сложных систем различны как по типу, так и по силе, что и позволяет, рассматривать эти системы как некоторую *совокупность взаимозависимых подсистем*. Внутренние связи элементов таких подсистем сильнее, чем связи между подсистемами. Так, компьютер состоит из процессора, памяти и внешних устройств, а Солнечная система включает Солнце и планеты, вращающиеся вокруг него. Используя то же различие связей, каждую подсистему можно аналогично разделить на подсистемы до «элементарного» уровня. На этом уровне система, состоит из немногих типов подсистем, по-разному скомбинированных и организованных. Иерархии такого типа получили название *«целое-часть»*.

В природе существует еще один вид иерархии - иерархия *«простое-сложное»* или иерархия *развития (усложнения) систем в процессе эволюции*. В этой иерархии любая функционирующая система является результатом развития более простой системы. Именно этот вид иерархии реализуется *механизмом наследования* объектно-ориентированного программирования.

Будучи отражением природных и технических систем, программные системы являются иерархическими и обладают описанными выше свойствами. На этих свойствах иерархических систем строится *блочно-иерархический подход* к их исследованию или созданию, предполагающий сначала создание частей объекта (блоков и модулей), а затем сборку из них самого объекта.

Процесс разбиения сложного объекта на сравнительно независимые части получил название *декомпозиции*. При декомпозиции учитывают, что связи между отдельными частями должны быть слабее, чем связи элементов внутри частей. Чтобы из полученных частей можно было собрать разрабатываемый объект, в процессе декомпозиции необходимо определить все виды связей частей между собой. Этот метод разработки получил название *пошаговой детализации*. В процессе декомпозиции стараются выделить аналогичные блоки, которые можно было бы разрабатывать на общей основе. Таким образом, обеспечивают увеличение степени повторяемости кодов и снижение стоимости разработки.

Вариант 5

Реализация файловых систем

Основными функциями файловой системы являются:

1) *Идентификация файлов* - связывание имени файла с выделенным ему пространством внешней памяти.

2) *Распределение внешней памяти между файлами* - для работы с конкретным файлом пользователю не требуется иметь информацию о местоположении этого файла на внешнем носителе информации.

3) *Обеспечение надежности и отказоустойчивости*.

4) *Обеспечение защиты от несанкционированного доступа.*

5) *Обеспечение совместного доступа к файлам.*

6) *Обеспечение высокой производительности*.

Надежность – одна из важнейших характеристик файловой системы, поскольку ее разрушение зачастую более опасно, чем разрушение компьютера. Поэтому файловые системы должны разрабатываться с учетом подобной возможности. Помимо своевременного *дублирования информации* (*backup*), файловые системы современных ОС содержат специальные средства для поддержки собственной совместимости.

Для надежной работы файловой системы важен *контроль ее целостности*. В результате файловых операций блоки диска могут считываться в память, модифицироваться и затем записываться на диск. Например, копирование файла предполагает выделение ему блоков диска, формирование индексного узла, изменение содержимого каталога и т. д. В течение короткого периода времени между этими шагами информация в файловой системе оказывается *несогласованной*. Если вследствие непредсказуемой остановки системы, на диске будут сохранены изменения только для части этих объектов (нарушена атомарность файловой операции), файловая система на диске может быть оставлена в *несовместимом* состоянии. В современных ОС предусмотрены меры, которые позволяют свести к минимуму ущерб от порчи файловой системы, а затем полностью или частично восстановить ее целостность. К ним относятся:

1) *Порядок выполнения операций*. Очевидно, что для правильного функционирования файловой системы значимость отдельных данных неравноценна. Искажение содержимого пользовательских файлов не приводит к серьезным (с точки зрения целостности файловой системы) последствиям, тогда как несоответствия в файлах, содержащих управляющую информацию (директории, индексные узлы, суперблок), могут быть катастрофическими. Поэтому должен быть тщательно продуман порядок выполнения операций со структурами данных файловой системы.

2) *Проверка целостности файловой системы при помощи утилит*. Если нарушение произошло, то для устранения проблемы несовместимости можно прибегнуть к *утилитам* (fsck, chkdsk, scandisk и др.), которые проверяют целостность файловой системы. Они могут запускаться после

загрузки или после сбоя и осуществляют многократное сканирование разнообразных структур данных файловой системы в поисках противоречий.

К сожалению, не существует средств, гарантирующих абсолютную сохранность информации в файлах, поэтому в ситуациях, когда целостность информации нужно гарантировать с высокой степенью надежности, прибегают к дорогостоящим *процедурам дублирования*.

Вариант 6

Вредоносное ПО

Вредоносное программное обеспечение, направленное на нарушение системы защиты информации от несанкционированного доступа можно классифицировать по следующим критериям:

Логическая бомба - используется для уничтожения или нарушения целостности информации, однако, иногда ее применяют и для кражи данных. Логическая бомба является серьезной угрозой, и информационная безопасность, например предприятия, не всегда способна справиться с подобными атаками, то есть, информационная безопасность предприятия подвергается не типовой угрозе, а непредсказуемой атаке, где главную роль играет человеческий фактор. Например, есть реальные случаи, когда предугадавшие свое увольнение программисты вносили в формулу расчета зарплаты сотрудников компании корректировки, вступающие в силу сразу после того, как фамилия программиста исчезает из перечня сотрудников фирмы. Делаем вывод, что ни программные средства защиты информации, ни физическая защита информации в этом случае на 100% сработать не может.

Троянский конь – это программа, запускающаяся к выполнению дополнительно к другим программным средствам защиты информации и прочего программного обеспечения, необходимого для работы.

То есть, троянский конь обходит систему защиты информации путем завуалированного выполнения недокументированных действий.

Такой дополнительный командный блок встраивается в безвредную программу, которая затем может распространяться под любым предлогом, а встроенный дополнительный алгоритм начинает выполняться при каких-нибудь заранее спрогнозированных условиях, и даже не будет замечен системой защиты информации, так как защита информации в сетях будет идентифицировать действия алгоритма, работой безвредной, заранее документированной программы. В итоге, запуская такую программу, персонал, обслуживающий информационную систему подвергает опасности компанию.

Вирус – это специальная самостоятельная программа, способная к самостоятельному распространению, размножению и внедрению своего кода в другие программы путем модификации данных с целью бесследного выполнения вредоносного кода. Существует специальная защита информации от вирусов.

Важно понимать, что обеспечение безопасности информационных систем от вирусных атак традиционно заключается в использовании такой службы защиты информации, как антивирусное ПО и сетевые экраны. Эти программные решения позволяют частично решить проблемы защиты информации.

Вариант 7

Хаотическое проектирование баз данных

В современной индустрии разработки программного обеспечения устоялось мнение, что определить требование к продукту перед началом проекта невозможно, и поэтому разработка должна быть адаптирована к их постоянному изменению. В результате появились процессы, основанные на итерациях. А что происходит в процессе итерационной разработки с базами данных? Изменение требований вынуждает корректировать схему базы данных, причем чаще всего это происходит непрозрачно, без анализа общей картины и зависимостей.

Фактически разработка баз данных сегодня ведется «заплаточным» методом, как во времена господства «водопадного» процесса, – в начале проекта «рисуется» некая модель базы, основанная на частичных требованиях, известных к данному моменту, затем генерируется физическая база данных, а дальше про модель забывают, производя изменения прямо в базе данных. Минусы такого подхода очевидны: обмен знаниями и понимание общей картины затруднены, а изменения непрозрачны, что приводит к очень большим убыткам. Современные разработчики приложений баз данных нуждаются в инструментах, приспособленных к итерационной разработке баз данных.

Первым и наиболее важным условием такой приспособленности является наличие полноценных возможностей *обратного инжиниринга* (reverse engineering, создание модели базы данных на основе анализа ее физической схемы) и *прямого инжиниринга* (forward engineering; создание и изменение физической схемы базы данных на основе модели). На практике это означает, что с помощью инструмента проектирования можно провести анализ схемы существующей базы данных, создать на ее основе модель базы, поменять модель и немедленно применить изменения, которые должны действительно корректно и непротиворечиво изменить схему базы данных, а не испортить или запутать ее.

Разработчики приложений редко работают в одиночку, поэтому нуждаются в средствах совместной работы, но если на стороне разработки приложений с этим все в порядке, то совместная работа над базой данных обычно никак не поддерживается на уровне инструментальных средств. Совместная работа обязательно предполагает систему контроля версий: все версии моделей и физической схемы базы данных должны сохраняться в едином репозитории (место в сети интернет, где хранятся какие-либо данные),

обеспечивая возможности отката и сравнения схем с самого начала процесса разработки.

Разработка баз данных – дело не менее важное, чем разработка приложений, поэтому стратегическим направлением развития является обеспечение процесса разработки баз данных средствами контроля версий и управления требованиями, а также явная привязка этапов моделирования и модифицирования баз данных к итерациям и меняющимся требованиям программного проекта.

Вариант 8

Защита информации

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации.

Под информационной безопасностью (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации.

Другими словами вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Виды информационной безопасности, а точнее виды угроз защиты информации условно подразделяются на пассивную и активную.

Пассивный риск информационной безопасности направлен на внеправовое использование информационных ресурсов и не нацелен на нарушение функционирования информационной системы. К пассивному риску информационной безопасности можно отнести, например, доступ к базе данных или прослушивание каналов передачи данных.

Активный риск информационной безопасности нацелен на нарушение функционирования действующей информационной системы путем целенаправленной атаки на ее компоненты.

К активным видам угрозы компьютерной безопасности относится, например, физический вывод из строя компьютера или нарушение его работоспособности на уровне программного обеспечения.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах

Вариант 9

Понятие информационной безопасности

Информационная безопасность – сравнительно молодая, быстро развивающаяся область информационных технологий. Словосочетание информационная безопасность в разных контекстах может иметь различный смысл. Состояние защищенности национальных интересов в информационной сфере определяется совокупностью сбалансированных интересов личности, общества и государства. Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности. С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий. Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры законодательного, административного, процедурного и программно-технического уровня. Информационная безопасность не сводится исключительно к защите от несанкцио- нированного доступа к информации, это принципиально более широкое понятие. Термин «компьютерная безопасность» (как эквивалент или заменитель ИБ) слишком узок. Компьютеры – только одна из составляющих информационных систем, и хотя внимание будет сосредоточено, в первую очередь, на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую

очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек. В определении ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне он ни рассматривался – национальном, отраслевом, корпоративном или персональном.

Вариант 10

Методы обеспечения информационной безопасности организации (фирмы)

Методами обеспечения защиты информации являются следующие: *препятствие, управление доступом, маскировка, регламентация, принуждение и побуждение.*

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. п.).

Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы организации (фирмы). Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

- аутентификацию (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

- регистрацию (протоколирование) обращений к защищаемым ресурсам;

- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

Маскировка – метод защиты информации в автоматизированной информационной системе путем ее криптографического закрытия.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при

которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Принуждение – такой метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – такой метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Следует отметить, что указанные выше методы обеспечения информационной безопасности организации (фирмы) реализуются на практике применением различных механизмов защиты, для создания которых используются следующие основные средства: физические, аппаратные, программные, аппаратно-программные, криптографические, организационные, законодательные и морально-этические.

Вариант 11

Физические средства обеспечения информационной безопасности организации (фирмы)

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Наряду с традиционными механическими системами при доминирующем участии человека разрабатываются и внедряются универсальные автоматизированные электронные системы физической защиты, предназначенные для охраны территорий, охраны помещений, организации пропускного режима, организации наблюдения; системы пожарной сигнализации; системы предотвращения хищения носителей.

Элементную базу таких систем составляют различные датчики, сигналы от которых обрабатываются микропроцессорами, электронные интеллектуальные ключи, устройства определения биометрических характеристик человека и т. д.

Для организации охраны оборудования, входящего в состав автоматизированной информационной системы предприятия, и перемещаемых носителей информации (дискеты, магнитные ленты, распечатки) используются:

- различные замки (механические, с кодовым набором, с управлением от микропроцессора, радиоуправляемые), которые устанавливают на входные двери, ставни, сейфы, шкафы, устройства и блоки системы;

- микровыключатели, фиксирующие открывание или закрывание дверей и окон;

- инерционные датчики, для подключения которых можно использовать осветительную сеть, телефонные провода и проводку телевизионных антенн;

- специальные наклейки из фольги, которые наклеиваются на все документы, приборы, узлы и блоки системы для предотвращения их выноса из помещения. При любой попытке вынести за пределы помещения предмет с наклейкой специальная установка (аналог детектора металлических объектов), размещенная около выхода, подает сигнал тревоги;

- специальные сейфы и металлические шкафы для установки в них отдельных элементов автоматизированной информационной системы (файл-сервер, принтер и т. п.) и перемещаемых носителей информации.

Вариант 12

Нейтрализация утечки информации

Для нейтрализации утечки информации по электромагнитным каналам используют экранирующие и поглощающие материалы и изделия.

При этом:

- экранирование рабочих помещений, где установлены компоненты автоматизированной информационной системы, осуществляется путем покрытия стен, пола и потолка металлизированными обоями, токопроводящей эмалью и штукатуркой, проволочными сетками или фольгой, установкой загородок из токопроводящего кирпича, многослойных стальных, алюминиевых или из специальной пластмассы листов;

- для защиты окон применяют металлизированные шторы и стекла с токопроводящим слоем;

- все отверстия закрывают металлической сеткой, соединяемой с шиной заземления или настенной экранировкой;

- на вентиляционных каналах монтируют предельные магнитные ловушки, препятствующие распространению радиоволн.

Для защиты от наводок на электрические цепи узлов и блоков автоматизированной информационной системы используют:

- экранированный кабель для внутристоечного, внутриблочного, межблочного и наружного монтажа;

- экранированные эластичные соединители (разъемы), сетевые фильтры подавления электромагнитных излучений;

- провода, наконечники, дроссели, конденсаторы и другие помехоподавляющие радио – и электроизделия;

- на водопроводных, отопительных, газовых и других металлических трубах помещают разделительные диэлектрические вставки, которые осуществляют разрыв электромагнитной цепи.

Для контроля электропитания используются электронные отслеживатели – устройства, которые устанавливаются в местах ввода сети переменного напряжения. Если шнур питания перерезан, оборван или перегорел, кодированное послание включает сигнал тревоги или активирует телевизионную камеру для последующей записи событий.

Для обнаружения внедренных «жучков» наиболее эффективным считается рентгеновское обследование. Однако реализация этого метода связана с большими организационными и техническими трудностями.

Таким образом, применение специальных генераторов шумов для защиты от хищения информации с компьютеров путем съема ее излучений с экранов дисплеев оказывает неблагоприятное воздействие на организм человека, что приводит к быстрому облысению, снижению аппетита, головным болям, тошноте. Именно поэтому они достаточно редко применяются на практике.

Вариант 13

Аппаратные средства обеспечения информационной безопасности организации (фирмы)

Аппаратные средства защиты – это различные электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками.

Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т. д.

Основные функции аппаратных средств защиты:

- запрещение несанкционированного (неавторизованного) внешнего доступа (удаленного пользователя, злоумышленника) к работающей автоматизированной информационной системе;

- запрещение несанкционированного внутреннего доступа к отдельным файлам или базам данных информационной системы, возможного в результате случайных или умышленных действий обслуживающего персонала;

- защита активных и пассивных (архивных) файлов и баз данных, связанная с необслуживанием или отключением автоматизированной информационной системы;

- защита целостности программного обеспечения.

Эти задачи реализуются аппаратными средствами защиты информации с использованием метода управления доступом (идентификация, аутентификация и проверка полномочий субъектов системы, регистрация и реагирование).

Для работы с особо ценной информацией организации (фирмы) производители компьютеров могут изготавливать индивидуальные диски с уникальными физическими характеристиками, не позволяющими считывать информацию. При этом стоимость компьютера может возрасти в несколько раз.

Часто практикуется хранение в некотором защищенном месте системы сигнатур важных объектов системы. Например, для файла в качестве сигнатуры может быть использовано сочетание байта защиты файла с его именем, длиной и датой последней модификации. При каждом обращении к файлу или в случае возникновения подозрений текущие характеристики файла сравниваются с эталоном.

Свойство аппаратной системы контроля доступа означает возможность реконструкции событий или процедур. Здесь речь идет о документировании исполняемых процедур, ведении журналов регистрации, а также о применении четких и недвусмысленных методов идентификации и проверки.

Следует отметить, что задачу контроля доступа при одновременном обеспечении целостности ресурсов надежно решает только шифрование информации.

Вариант 14

Программные средства защиты

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития.

В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, включающих разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т. п.);

- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;

- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);

- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;

- защита информации от компьютерных вирусов;

- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;

- стирание остаточной конфиденциальной информации на магнитных дисках, выдача протоколов о результатах стирания;

- обеспечение целостности информации путем введения избыточности данных;

- автоматический контроль над работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

В настоящее время ряд операционных систем изначально содержит встроенные средства блокировки «повторного использования». Для других типов операционных систем существует достаточно много коммерческих программ, не говоря уже о специальных пакетах безопасности, реализующих аналогичные функции.

Вариант 15

Источники угроз информационной безопасности государства

Источники угроз информационной безопасности подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов в информационной сфере;

- стремление ряда стран к доминированию и ущемлению интересов государства в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

- обострение международной конкуренции за обладание информационными технологиями и ресурсами;

- деятельность международных террористических организаций;

- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира.

Внутренними источникам угрозы информационной безопасности являются:

- критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка страны;

- недостаточная экономическая мощь государства;

- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности.

- отставание государства от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Вариант 16

Объект и предмет правового обеспечения информационной безопасности

Одной из важных тенденций развития современного общества является интенсивное распространение современных информационных технологий, существенное усиление их влияния на все сферы общественной жизни и, как следствие, появление признаков перехода некоторых стран мира к новому этапу своего развития, получившему название «глобальное информационное общество».

Представляется, что основным признаком этого этапа развития является такое развитие экономики, при котором основная или значительная часть валового продукта производится за счет создания и внедрения наукоемких технологий, производства информационных продуктов и услуг, интеллектуального труда граждан.

Основными объектами правового обеспечения безопасности в информационной сфере являются:

- общественные отношения, которые, с одной стороны, имеют предметами составляющие этой сферы – субъектов информационной сферы, информацию и информационную инфраструктуру, а с другой – представляются важными для достижения национальных интересов в информационной сфере;

- внешние и внутренние угрозы общественным отношениям в информационной сфере, могущие нанести ущерб предметам и интересам субъектов этих отношений и, как следствие, – нанести ущерб национальным интересам государства в информационной сфере.

Фактическая деятельность государства в этой области направлена на разработку, принятие и применение юридических норм, регулирующих общественные отношения в информационной сфере в целях достижения соответствующих национальных интересов и их защиты от угроз.

Объектами правового обеспечение деятельности системы органов власти в области обеспечения информационной безопасности являются общественные отношения, возникающие при образовании, функционировании и прекращении деятельности этих органов государства, реализацией ими властных полномочий, организацией взаимодействия между ними, а также с гражданами и общественными организациями. Предметом этого вида правового обеспечения выступают методы и средства правового регулирования выделенных отношений в целях обеспечения эффективного функционирования механизма государства.

Правовое обеспечение безопасности в информационной сфере представляет собой деятельность государства и общества, осуществляемую в процессе подготовки и принятия норм права, их реализации в конкретных правоотношениях и применения государственного принуждения к правонарушителям.

Исходя из этого, можно отметить то, что особое место в правовом регулировании занимают правовые нормы, совокупность которых образует нормативное правовое обеспечение информационной безопасности.

Вариант 17

Защита информации в компьютерных сетях

Одним из методов защиты информации является создание физической преграды пути злоумышленникам к защищаемой информации (если она хранится на каких-либо носителях).

Управление доступом - эффективный метод защиты информации, регулирующий использование ресурсов информационной системы, для которой разрабатывалась концепция информационной безопасности.

Методы и системы защиты информации, опирающиеся на управление доступом, включают в себя следующие функции защиты информации в локальных сетях информационных систем:

- идентификация пользователей, ресурсов и персонала системы информационной безопасности сети;
- опознание и установление подлинности пользователя по вводимым учетным данным (на данном принципе работает большинство моделей информационной безопасности);
- допуск к определенным условиям работы согласно регламенту, предписанному каждому отдельному пользователю, что определяется средствами защиты информации и является основой информационной безопасности большинства типовых моделей информационных систем;
- протоколирование обращений пользователей к ресурсам, информационная безопасность которых защищает ресурсы от несанкционированного доступа и отслеживает некорректное поведение пользователей системы.

Различают 4 уровня защиты информации:

- предотвращение - доступ к информации и технологии только для персонала, который имеет допуск от собственника информации;
- обнаружение - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены;
- ограничение - уменьшается размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению;
- восстановление - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Когда компьютеры впервые появились, они были доступны только небольшому числу людей, которые умели их использовать. Обычно они помещались в специальных помещениях, удаленных территориально от помещений, где работали служащие.

Сегодня все изменилось. Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное преступление можно предотвратить, а ущерб от возможного нарушения системы информационной безопасности можно сделать минимальным, если внимательно анализировать систему информационной безопасности на уязвимость и предпринимать меры для укрепления обнаруженных уязвимых мест.

Вариант 18

Индивидуальность и конфиденциальность

Распространение устройств доступа к сетям, в особенности, связанных беспроводными технологиями, дает использование сетей повсеместным и многообразным, создает возможности для бизнеса и общества. Сегодняшние сетевые платформы вносят значительный вклад в развитие

сервис-ориентированной экономики. В число этих сервисов входит поддержка автоматизированных транзакций, для выполнения которых требуется безошибочный и надежный обмен информацией между участниками транзакции.

Для управления транзакциями и настройки сервисов обычно используется учетная информация об участнике транзакции (имя и связанные с ним индивидуальные атрибуты, включающие биометрические данные), которая позволяет формировать и передавать данные за пределы административных границ. Использование атрибутов, идентифицирующих конкретного индивидуума и составляющих его «цифровую личность», является неотъемлемой частью служб сетевых транзакций, в которых участвуют правительственные и коммерческие организации, а также отдельные люди. Однако при этом часто не учитывают, что для учетной информации нужны «доверительные якоря» (trust anchor).

В отличие от реального мира, для киберпространства характерно исчезновение границ, которые в прошлом служили естественной защитой от утечки персональной информации. Тенденция к переносу повседневной жизни и деловой активности на территорию Internet раскрывает людей в значительно большей степени, чем это было возможно когда бы то ни было раньше – сегодня крупнейшая в мире сетевая инфраструктура, включающая значительные компоненты *управления учетной информацией* (Identity Management, IdM), поддерживает мобильную телефонию.

Доступность недорогих и легко осваиваемых технологий перехвата и интеллектуального анализа данных облегчает использование учетных данных в злонамеренных целях. Проблема краж учетной информации уже стала одной из центральных для правительственных, общественных и коммерческих организаций. Повсеместное внедрение систем для сбора, обработки и совместного использования информации, идентифицирующей конкретных индивидуумов, для поддержки сервисов, делает онлайновые кражи учетных данных нередким явлением, что подрывает доверие к ИТ. Это приводит к расширению области исследований, затрагивающих несколько тем IdM, включая совершенствование достоверности и конфиденциальности учетной информации.

Вариант 19

От чего или кого защищаться в Интернете?

Мошенники были всегда и везде. Они каждый раз придумывали новые способы вытягивания денег с простых людей. В интернете таких людей прозвали "Хакеры".

Хакеры используют вирусы, чтобы проникнуть на ваш компьютер и получить доступ к вашей личной информации.

Что я имею ввиду под личной информацией?

- логины и пароли от социальных сетей и от электронного почтового ящика;
- пароли от электронных кошельков;
- банковские реквизиты;
- пароли от интернета.

Вся эта информация нужна хакерам для распространения своего вируса вашим знакомым и друзьям, ну и естественно для того, чтобы обогатиться.

Какими способами используют хакеры?

1. Заражение вирусами. Благодаря вирусу мошенник может проникнуть в ваш компьютер и украсть всю вашу личную информацию с него.
2. Кейлоггер (англ. keylogger) – представляет из себя маленькую программу, которая способна считывать нажатие клавиш и после передавать собранную информацию о логинах и паролях хакеру.
3. Радмин (англ. Radmin) или неправомерный доступ. Ну тут как говорится, смотря в чьи руки он попадет. Если программа попала в добрые руки, то с ее помощью людям оказывают удаленную техническую поддержку, администрирование компьютером. В злых руках работает как вирус, т.е. ищет нужную мошенникам информацию.

Кстати, вот ссылка на официальный сайт Radmin http://www.radmin.ru/. Если перейдете по ссылке, то можете увидеть, что данная программа создана для удаленной технической поддержки сотрудников. Можете скачать, кого заинтересовала программа и не бояться, что вас взломают.

Radmin работает в режиме защиты данных, при котором все передаваемые данные, изображения экрана, перемещение курсора и сигналы клавиатуры надёжно защищены. Секретный ключ генерируется случайным образом для каждого подключения.

Мошенничество. Когда под видом одного сайта вы заходите на сайт мошенников, и они просят вас отослать на короткий номер телефона СМС или, допустим, устанавливаете приложение для сотового, после чего деньги начинают исчезать с него.

Вот такое оружием пользуется хакер в наше время.

Итак, мы познакомились с нашим противником, и узнали чем он вооружен.

Как говорится "Предупреждён – значит вооружён".

Вариант 20

Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

- физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов

компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

- внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

- вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

- применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления и т.п.);

- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

- несанкционированное копирование носителей информации;

- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

- вскрытие шифров криптозащиты информации;

- незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений и т.д.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Вариант 21

Понятие электронной цифровой подписи

В условиях увеличившегося числа преступлений в информационной сфере, необходимы перемены в сфере информационных технологий. Одной из

новых технологий, обеспечивающих безопасность информации, является электронная цифровая подпись.

Для наилучшего понимания данной информации необходимо уделить внимание следующим понятиям.

Электронное сообщение – информация, представленная в форме набора состояний элементов электронной вычислительной техники, иных электронных средств обработки, хранения и передачи информации, могущей быть преобразованной в форму, пригодную для однозначного восприятия человеком.

Документ в электронной форме отображения (электронный документ) – электронное сообщение, имеющей атрибуты для идентификации его как документа.

Электронная цифровая подпись (ЭЦП) – последовательность символов, полученная в результате криптографического преобразования исходной информации с использованием закрытого ключа ЭЦП, которая позволяет пользователю открытого ключа ЭЦП, установить целостность и неизменность этой информации, а также владельца закрытого ключа ЭЦП.

Средство ЭЦП – совокупность программных и технических средств, реализующих функцию выработки и проверки ЭЦП.

Открытый ключ ЭЦП – общедоступная последовательность символов, предназначенная для проверки ЭЦП.

Закрытый ключ ЭЦП – последовательность символов, предназначенная для выработки ЭЦП и известная только правомочному лицу.

Пользователь открытого ключа ЭЦП – физическое или юридическое лицо, использующее открытый ключ ЭЦП.

Сертификат открытого ключа ЭЦП (сертификат ключа подписи) – документ, выданный и заверенный удостоверяющим центром, подтверждающий принадлежность открытого ключа ЭЦП определенному лицу.

Владелец сертификата ключа подписи (владелец сертификата) – физическое или юридическое лицо, на имя которого выдан сертификат ключа подписи, и которое владеет закрытым ключом ЭЦП, соответствующим открытому ключу, указанному в сертификате.

Сертификат на средство ЭЦП – документ, выданный по правилам соответствующей системы сертификации, удостоверяющий соответствие этого средства специальным требованиям и гарантирующий в течение определенного срока действия возможность использования данного средства в качестве инструмента выработки и проверки ЭЦП.

Подтверждение подлинности ЭЦП – положительный результат проверки правильности ЭЦП, выработанной правомочным лицом из исходной информации путем применения принадлежащего ему закрытого ключа ЭЦП, полученный с использованием зарегистрированного и сертифицированного открытого ключа ЭЦП.

Вариант 22

Пути решения проблем защиты информации в сетях

Для поиска решений проблем информационной безопасности при работе в сети Интернет был создан независимый консорциум ISTF (Internet Security Task Force) – общественная организация, состоящая из представителей и экспертов компаний-поставщиков средств информационной безопасности, электронных бизнесов и провайдеров Internet-инфраструктуры. Цель консорциума – разработка технических, организационных и операционных руководств по безопасности работы в Internet.

Консорциум ISTF выделил 12 областей информационной безопасности. Этот список, в частности, включает:

- аутентификацию (механизм объективного подтверждения идентифицирующей информации);
- право на частную, персональную информацию (обеспечение конфиденциальности информации);
- определение событий безопасности (Security Events);
- защиту корпоративного периметра;
- определение атак;
- контроль за потенциально опасным содержимым;
- контроль доступа;
- администрирование;
- реакцию на события (Incident Response). Рекомендации ISTF предназначены для существующих или вновь образуемых компаний электронной коммерции и электронного бизнеса.

Их реализация означает, что защита информации в системе электронного бизнеса должна быть комплексной.

Для комплексной зашиты от угроз и гарантии экономически выгодного и безопасного использования коммуникационных ресурсов для электронного бизнеса необходимо: проанализировать угрозы безопасности для системы электронного бизнеса; разработать политику информационной безопасности; защитить внешние каналы передачи информации, обеспечив конфиденциальность, целостность и подлинность передаваемой по ним информации; гарантировать возможность безопасного доступа к открытым ресурсам внешних сетей и Internet, а также общения с пользователями этих сетей; предоставить персоналу защищенный удаленный доступ к информационным ресурсам корпоративной сети; обеспечить надежное централизованное управление средствами сетевой защиты.

Таким образом, согласно рекомендациям ISTF, первым и важнейшим этапом разработки системы информационной безопасности электронного бизнеса являются механизмы управления доступом к сетям общего пользования и доступом из них, а также механизмы безопасных коммуникаций, реализуемые МЭ и продуктами защищенных виртуальных сетей VPN.

Сопровождая их средствами интеграции и управления всей ключевой информацией системы защиты (PKI - инфраструктура открытых ключей), можно получить целостную, централизованно управляемую систему информационной безопасности.

Вариант 23

Стандарты информационной безопасности

Главная задача стандартов информационной безопасности – создать основу для взаимодействия между производителями, потребителями и экспертами по квалификации продуктов ИТ. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности. Потребители также нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения. К сожалению, многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т. д.), вынуждают отказаться от широко распространенных и незащищенных прикладных программных средств.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя требования безопасности должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д.

Эксперты по квалификации и специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами ИТ, и предоставить потребителям возможность сделать обоснованный выбор. Эксперты по квалификации находятся в двойственном положении: с одной стороны, они, как и производители, заинтересованы в четких и простых критериях, над которыми не надо ломать голову, как их применить к конкретному продукту, а с другой стороны, они должны дать обоснованный ответ пользователям – удовлетворяет продукт их нужды или нет.

Таким образом, перед стандартами информационной безопасности стоит непростая задача – примирить три разные точки зрения и создать эффективный механизм взаимодействия всех сторон. Причем ущемление

потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу – создание защищенной системы обработки информации.

Вариант 24

Технологии защиты межсетевого обмена данными

Развитие глобальных компьютерных сетей, появление новых перспективных информационных технологий (ИТ) привлекают все большее внимание. Глобальные сети применяются для передачи коммерческой информации различного уровня конфиденциальности, например для связи головной штаб-квартиры организации с удаленными офисами или создания Web-сайтов организации с размещенной на них рекламой и деловыми предложениями. Многие организации принимают решение о подключении своих локальных и корпоративных сетей к открытой глобальной сети.

Однако подключение к открытой глобальной сети может иметь и негативные последствия, поскольку появляются угрозы неправомерного вторжения из внешней сети во внутреннюю сеть. Такое вторжение может выполняться как с целью несанкционированного использования ресурсов внутренней сети, например, хищения информации, так и с целью нарушения ее работоспособности. Количество уязвимостей сетевых операционных систем (ОС), прикладных программ и возможных атак на количество информационных систем (КИС) постоянно растет. Без соответствующих средств защиты вероятность успешной реализации таких угроз является достаточно высокой.

Ежегодные потери, обусловленные недостаточным уровнем защищенности компьютерных сетей организаций, оцениваются миллиардами долларов. Поэтому при подключении к Internet локальной или корпоративной сети необходимо позаботиться об обеспечении информационной безопасности этой сети.

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных компьютерных сетей. К базовым средствам многоуровневой защиты межсетевого обмена данными относятся защищенные ОС, МЭ, виртуальные защищенные сети VPN, протоколы защиты на канальном, транспортном и сетевом (протокол IPSec) уровнях.

Таким образом, большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка ОС. Окружение, в котором функционирует ОС, называется *доверенной вычислительной базой* (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: ОС, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная ОС.

Семестровая работа студента № 3

Тема: виды и способы развития информации в тексте.

Цель: применить на практике знания о видах информации в научном тексте.

Распределение вариантов остаётся согласно выполненной ранее СРС №2.

Задачи работы:

- в каждой микротоме (МТ) текста указать основную и виды дополнительной информации;
- составить толковый терминологический словарь к анализируемому тексту;
- пересказать текст.

Семестровая работа студента № 4

Тема: аннотирование научного текста.

Цель: закрепить навыки составления аннотации.

Задачи работы:

- подобрать текст из учебно-научной литературы по своей специальности объемом 7-8 страниц (смотри рекомендательный список);
- составить толковый словарь узкоспециальных терминов, содержащихся в выбранном тексте (не менее 10 терминов);
- написать аннотацию текста (приложить оттиск выбранного текста).

Примерный перечень вариантов, рекомендуемых для выполнения СРС № 4

(В книге Дейт, К. Дж. Введение в системы баз данных. Пер.: с англ. – М.: Издательский дом «Вильяме», 2005, 2006. – 1328 с.).

1. Общее определение и назначение баз данных (с. 43 – 58).
2. Архитектура системы базы данных (с. 75 – 90).
3. Система управления передачей данных (с. 91 – 95).
4. Введение в реляционные базы данных (с. 103 – 113).
5. Введение в язык SQL (с. 133 – 154).
6. Типы данных (определение значений и переменных) (с. 165 – 175).
7. Реляционное исчисление (с. 289 – 295).
8 Целостность данных (с. 375 – 377).
9. Обновление данных в представлениях (с. 400 – 412).
10. Операция соединения (с. 415 – 421).
11. Проектирование базы данных (с. 433 – 437).
12. Функциональные зависимости (с. 438 – 451).
13. Нормальные формы (с. 459 – 475).
14. Семантическое моделирование (с. 531 – 540).

15. Краткий анализ ER-модели (с. 548 – 553).

16. Управление транзакциями. Восстановление (с. 573 – 591).

17. Параллельность. Три проблемы организации параллельной работы (с. 599 – 610).

18. Уровни изоляции (с. 618 – 624).

19. Защита данных (с. 647 – 660).

20. Распределенные базы данных (с. 821 – 859).

(В книге Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 4-е издание. – М.: Изд.»Академия», 2009. 336 с.).

1. Информационные геополитические и экономические процессы современного общества (с. 10 – 29).

2. Комплексное обеспечение информационной безопасности государства (с. 29 – 43).

3. Организационные, физико-технические, информационные угрозы (с. 43 – 50).

4. Организационное и правовое обеспечение информационной безопасности (с. 52 – 63).

5. Организационная защита переработки информации (с. 63 – 71).

6.Современные подходы к обеспечению решения проблем ИБ деятельности общества (с. 75 – 85).

7. Методология информационного противоборства (с. 85 – 96).

8. Информационно-манипулятивные технологии (с. 97 – 106).

9. Области и сферы обеспечения ИБ предприятий и организаций (с. 106 – 117).

10. Методы и средства предотвращения случайных угроз КС (с. 130 – 147).

11. Методы и средства нейтрализации угроз (с. 149 – 158).

12. Методологические основы технического обеспечения защиты информации (с. 158 – 169).

13. Комплексный и системный подходы к обеспечению ИБ объектов (с. 176 – 189).

14. Общие вопросы организации противодействия информационной и технической агрессии (с. 189 – 200).

15. Программно-аппаратные средства защиты ПЭВМ (с. 202 – 220).

16. Классификация компьютерных вирусов (с. 223 – 230).

17. Методы и технологии борьбы с компьютерными вирусами (с. 231 – 240).

18. Защита процессов переработки информации в СУБД (с. 245 – 256).

19. Программно-аппаратные средства обеспечения ИБ в вычислительных сетях (с. 277 – 286).

20. Защита процессов переработки информации в Интернете и Интранете (с. 298 – 327).

(В книге Чекмарев Ю.В. Вычислительные системы, сети и телекоммуникации. Изд. 2-е, исправленное и дополненное. - М.: ДМК Пресс, 2009. – 184 с.).

1. Общие сведения о вычислительных системах, сетях и телекоммуникациях (с. 6 – 15).

2. Физические основы вычислительных процессов (с. 18 – 24).

3. Организация передачи данных. Защита от ошибок (с. 25 – 32).

4. Основы построения и функционирования вычислительных машин (с. 34 – 40).

5. Системы счисления. Представление информации в ЭВМ (с. 40 – 48).

6. Функциональная и структурная организация ЭВМ (с.49 – 58).

7. Периферийные устройства (с. 58 – 65).

8. Внешние устройства. Программное обеспечение (с. 65 – 74).

9. Развитие и перспективы ЭВМ (с. 75 – 79).

10 Многомашинные и многопроцессорные вычислительные системы (с. 81 – 87).

11. Техническое и информационное обеспечение ВС (с. 89 – 93).

12. Программное обеспечение ВС (с. 93 – 97).

13. Архитектура ВС (с. 97 – 104).

14. Структура и характеристика систем телекоммуникаций (с. 105 – 111).

15. Протоколы передачи данных нижнего уровня (с. 111 – 117).

16. Цифровые сети связи (с. 117 – 126).

17. Понятие эффективности ТВС и методология ее оценки (169 – 173).

18. Перспективы развития вычислительных средств (с. 178 – 183).

19. Персональные ЭВМ (с. 34 – 44).

20. Различные сети и технологии ТКС (с. 134 – 160).

Семестровая работа студента № 5

Тема: реферирование.

Цель: презентация обзорного информативного реферата.

Задачи работы:

- определить тему обзорного реферата из предложенного списка (15 тем);
- подобрать необходимую литературу для раскрытия темы;
- написать реферат на основании сопоставления, сравнения и обобщения разных источников;
- сделать презентацию своей работы.

Темы, рекомендуемые для выполнения СРС 5 специальности 5В070400 – Вычислительная техника и программное обеспечение

1. Лазерные технологии в вычислительной технике.
2. Наука и техника, в чем их взаимосвязь.
3. Профессия инженера вчера, сегодня, завтра.
4. Человек и машина: история взаимоотношений.
5. Прорывные технологии в вычислительной технике.
6. Культура пользователя современными вычислительными машинами.
7. Лазеры в медицине – все преимущества и недостатки.
8. Если разобрать компьютер…
9. IBM – мировой лидер в сфере вычислительной техники.
10. Искусственный интеллект и человеческий разум.
11. Мой компьютер – мой друг/враг.
12. Компьютерные игры. Виртуальность и реальная жизнь.
13. Предприятия и организации Республики Казахстан и используемые ими локальные вычислительные сети.
14. О разработке системы учета и оплаты проезда в общественном транспорте в г.Алматы «Оңай»: достоинства и недостатки.
15. Система электронного документооборота в г.Алматы: уровень доступности и качества.
16. Применение объектно-ориентированного анализа при разработке сложных технических систем.
17. О языках объектно-ориентирования моделирования (SIMULA-67, ObjectMath, Omola, Modelica).

Темы, рекомендуемые для выполнения СРС 5 специальности 5В100200 – Системы информационной безопасности

1. IT-специалисты Казахстана, их конкурентоспособность в мировом сообществе.
2. Проблема информационной защищенности личной жизни граждан от нежелательного вторжения.
3. Охранные системы в быту, на производстве, в бизнесе.
4. Каково влияние радиоизлучения на здоровье человека.
5. Прорывные технологии в информационной безопасности.
6. Национальная безопасность и защита информации.
7. Уровень информационной безопасности на сегодня.
8. Какие средства защиты информации мы знаем, их плюсы и минусы.
9. Защита информации в компьютерных системах.
10. Какие средства информационной безопасности на мировом рынке наиболее востребованны?
11. Пути усовершенствования службы оповещения населения о ЧС г.Алматы.

12. Как повысить уровень надежности информационной безопасности банковской сферы г.Алматы.

13. Место и роль информационной безопасности в различных сферах жизнедеятельности личности.

14. Несанкционированный вход в информационную систему. (хакерство) как явление в профессиональной сфере IT-технологий.

15. Сравнительный анализ методов информационного противостояния (противоборства) и способы их использования.

16. Системы кодирования речи от Морзянки до ….

Список периодических изданий, рекомендуемых для отбора статьи

1. Техника молодежи//Санкт-Петербург: Изд.ООО «Девиз», 2015.
2. Информационные технологии//М.: Изд.«Новые технологии», 2014.
3. Computerword Россия// М.: Изд. «Открытые системы», 2015.
4. Информационная безопасность//М.:Изд. «Groteck», 2015.
5. Мир ПК//Москва, Россия, 2015.
6. Наука и жизнь//М.: «Наука и жизнь», 2015.
7. Инженер//М.: ГУП МО КТ «Раменская типография», 2015.
8. Знание сила//М.: АО «Первая образцовая типография», 2015.

Семестровая работа студента № 6

Тема: содержание этики речевого поведения в деловой коммуникации.

Цель: демонстрация владения образцами речевого этикета в деловой сфере.

Задачи работы:

1) выбрать тему из предложенных вариантов;
2) составить словарь ситуативно-речевых образцов (не менее 20-ти единиц);
3) предъявить знание формул этикетов в устном диалоге с преподавателем.

Темы, рекомендуемые для выполнения СРС 6

1. Собеседование при приеме на работу по специальности после окончания вуза.
2. Отборочное собеседование перед творческим конкурсом.
3. Разговор с директором фирмы, давшей объявление о наборе инженеров.
4. Разговор с ректором университета с целью добиться разрешения перейти на другой факультет.

5. Разговор с руководителем отдела (цеха, лаборатории) о повышении должностного оклада.

6. Беседа с деканом факультета о кредитной системе обучения в Казахстане.

7. Разговор студента с эдвайзером о непосещении занятий.

8. Староста обращается с просьбой к преподавателю о продлении срока сдачи СРС.

9. Студент берет интервью у декана факультета.

10. Разговор с организатором курсов по вождению автомобиля, на которых вы хотели бы заниматься, несмотря на то, что прошло две недели после начала занятий.

Приложение А

Образец титульного листа

НАО «АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
КАФЕДРА КАЗАХСКОГО И РУССКОГО ЯЗЫКОВ

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА № 4

Дисциплина: «Русский язык»

Тема: аннотирование научного текста

Специальность: 5В081200 – Энергообеспечение сельского хозяйства

Выполнил (а): Бауржанулы М. Группа: ЭСХк-15-03

Проверил (а): Курманбаева Т.С.

_____ _____ « » _____ 2016 г.
оценка подпись

Алматы 2016

Список литературы

1 Вычислительные машины системы и сети Конспект лекций// составитель Ю.В.Шевяков.- А.: «АУЭС», 2007.

2 Даль В.И. Большой иллюстрированный толковый словарь русского языка: современное написание. Около 1500 илл. – М.: «АСТ – Астрель - Хранитель», 2008. – 352 с.

3 Журнал «Системы безопасности», № 5,6,7. – 2008.

4 Коржымбаев Т.Т., Нурмагамбетов Г.С. Конспект лекций по дисциплине «Организация вычислительных систем и сетей» для студентов 5В07400. – Алматы: АУЭС, 2013. – 67 с.

5 Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 4-е издание. – М.: Изд. «Академия», 2009. – 336 с.

6 Мухамадиев Х.С. Пособие по научному стилю речи: для казахских отделений университета. -3-е изд. – Алматы: Қазақ университеті, 2011.- 210 с.

7 Русский язык: учебное пособие для студентов казахских отделений университета (бакалавриат)/ Под ред. К.К.Ахмедьярова, Ш.К.Жаркынбековой. –Алматы: Қазақ университеті, 2009.– 226 с.

8 Саньярова Н.С., Турбекова С.А. Профессиональный русский язык в техническом вузе (учебное пособие для студентов специальности 5В070400 – Вычислительная техника и программное обеспечение): Учебное пособие. - Алматы: КазНТУ.2014.- 200 с.

9 Смирнова Ю.Г. Русский язык-1. Научный стиль. Дидактические материалы для языковой и речевой подготовки (для специальности 5В070400 – Вычислительная техника и программное обеспечение). – Алматы: АУЭС, 2011. – 82 с.

10 Ташимов М.А. Современные вычислительные системы и сетевые технологии. – Алматы: Изд. ТОО «Print-S», 2004. – 384 с.

11 Теория информационных процессов и систем: Учебник для студентов высш.учеб.завед./под ред.Б.Я.Советова. – М.: Изд.центр «Академия», 2010. – 432 с.

12 Тойгожинова А.Ж., Тергеусизова А.С. Компьютерные сети. Конспект лекций для студентов специальности 5В07400 – Вычислительная техника и программное обеспечение. – Алматы: АУЭС, 2014. – 69 с.

13 Тусипбек М.Р., Кусаинов А.К. Русско-казахско-английский политехнический словарь: в 2-х томах. – Алматы: Rond&A, 2010.

14 Федосюк, М.Ю. и др. Русский язык для студентов-нефилологов [Текст]: Учебное пособие/М.Ю. Федосюк. – 4-е изд. – М.: Флинта: Наука, 2000. – 256 с.

15 Филин С.А. Информационная безопасность. Учебное пособие. - М.: Альфа-Пресс, 2006.

16 Чекмарев Ю.В. Вычислительные системы, сети и телекоммуникации. Изд. 2-е, исправленное и дополненное. - М.: ДМК Пресс, 2009. – 184 с.

17 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учеб.пособие. – М.: ИД «Форум»: ИНФРА-М, 2011. – 416 с.
Техника молодежи//Санкт-Петербург: Изд.ООО «Девиз», 2015.
18 Информационные технологии.- М.: Изд.«Новые технологии», 2014.
19 Computerword Россия. - М.: Изд.»Открытые системы», 2015.
20 Информационная безопасность. - М.:Изд. «Groteck», 2015.
21 Мир ПК. - Москва, Россия, 2015.
22 Наука и жизнь. - М.: «Наука и жизнь», 2015.
23 Инженер. - М.: ГУП МО КТ «Раменская типография», 2015.
24 Знание сила. - М.: АО «Первая образцовая типография», 2015.

Содержание

Сводный план 2015 г., позиция 67

Курманбаева Толганай Сагыновна

РУССКИЙ ЯЗЫК

Методические указания и варианты семестровых работ для студентов специальностей 5В070400, 5В100200

Редактор Н.М. Голева
Специалист по стандартизации Н.К. Молдабекова

Подписано в печать __.__.__ Формат 60х84 1/16
Тираж 50 экз. Бумага типографская №1
Объем 4,1 уч.__изд.л. Заказ__ цена 2050 тенге

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики и связи»
050013, Алматы, Байтурсынова,126